(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08083205 A**

(43) Date of publication of application: **26 . 03 . 96**

(51) Int. Cl **G06F 12/00**
G06F 12/14
G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21) Application number: **06252623**

(22) Date of filing: **09 . 09 . 94**

(71) Applicant: **FUJITSU LTD**

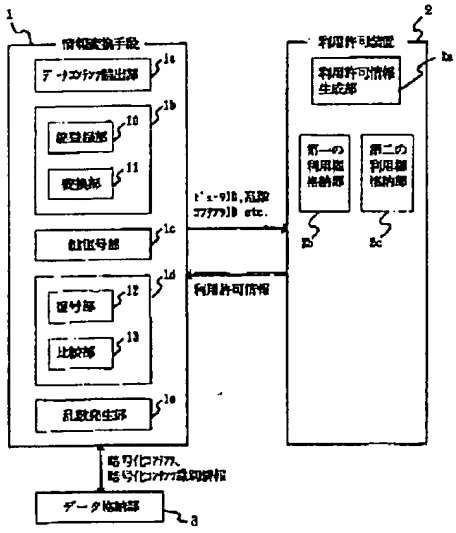
(72) Inventor: **IWAYAMA NOBORU**
TORII NAOYA
HASEBE TAKAYUKI
TAKENAKA MASAHIKO
MATSUDA MASAHIRO

(54) **DATA CONTENT UTILIZATION SYSTEM**

(57) Abstract:

PURPOSE: To prevent software from illegally being used, to improve the security of software utilization, and to increase the flexibility of charging management by providing a specific data storage part, an information converting means, and a utilization permitting device.

CONSTITUTION: The data storage part 3 stores at least one kind of information which indicates a medium, such as a CD-ROM, storing software or an area on the medium where data are stored and generated by ciphering data contents and content discrimination information specifying the individual data contents. The information converting means 1 is equipped with a function which outputs data contents that a user desires as visual and auditory data, a function which prevents the data contents from being put in a file, and a function which deciphers the ciphered information. Further, the utilization permitting device 2 has a function which generates utilization permit information for the data contents stored in the data storage part 3.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－83205

(43)公開日　平成8年(1996)3月26日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/00	５３７　Ａ	7623－5B		
	12/14	３２０　Ａ			
Ｇ０９Ｃ	1/00		7259－5Ｊ		
Ｈ０４Ｌ	9/00				
				Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数18　書面　(全 30 頁)　最終頁に続く

(21)出願番号　特願平6－252623

(22)出願日　平成6年(1994)9月9日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　岩山　登
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　鳥居　直哉
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　遠山　勉　(外１名)

最終頁に続く

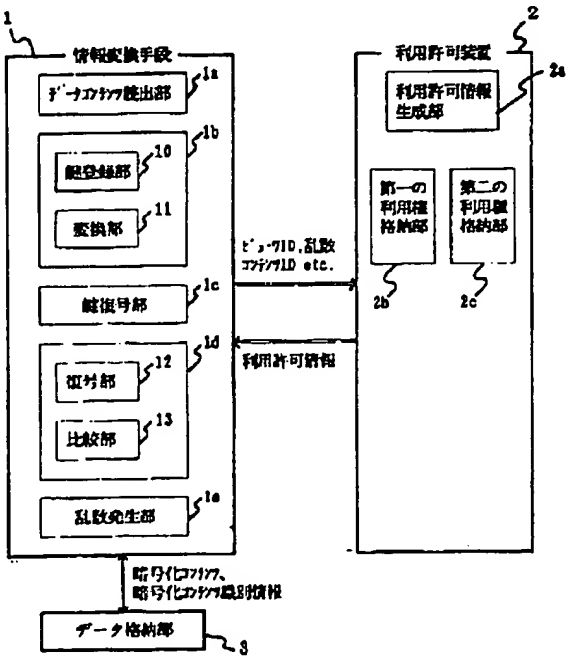
(54)【発明の名称】　データコンテンツ利用システム

(57)【要約】

【目的】　データコンテンツをユーザへ提供するシステムにおいて、データコンテンツ利用にかかるセキュリティーチェックの向上を図ると共に、データコンテンツ利用にかかる課金管理を柔軟に行える技術を提供することを目的とする。

【構成】　データコンテンツとコンテンツ識別情報とを暗号化してなる情報を平文形式のコンテンツ識別情報毎に格納するデータ格納手段と、このデータ格納手段からユーザが希望する情報を読み出し、利用許可装置から提供される利用許可情報に基づいて復号して可視的・可聴的なデータとして出力する情報変換手段と、前記情報変換手段固有の情報に基づいて前記データコンテンツの利用許可情報を生成する利用許可装置とから構成されるデータコンテンツ利用制御方式。

第一の発明の原理図



1

【特許請求の範囲】

【請求項１】　データコンテンツとこのデータコンテンツを特定するコンテンツ識別情報とを暗号化してなる情報を格納するデータ格納手段と、
ユーザが希望するデータコンテンツを可視的・可聴的なデータとして出力する情報変換手段と、
前記データコンテンツの利用許可情報を生成する利用許可装置とを備え、
前記情報変換手段は、ユーザが希望するデータコンテンツを前記データ格納部から読み出すデータコンテンツ読出部と、
前記情報変換手段を識別する情報変換手段識別情報に基づいて鍵復号鍵を生成する鍵生成部と、
前記鍵生成部の生成した鍵復号鍵及び前記利用許可装置から取得する利用許可情報に基づいて前記暗号化データコンテンツを復号するための復号鍵を生成する鍵復号部と、
前記データコンテンツ読出部が読み出した暗号化データコンテンツを前記鍵復号部が生成した復号鍵に基づいて復号するデータ復号部とを具備し、
前記利用許可装置は、前記情報変換手段から少なくとも情報変換手段識別情報とコンテンツ識別情報とを受け取り、これらの情報に基いて利用許可情報を生成する利用許可情報生成部を具備することを特徴とするデータコンテンツ利用システム。

【請求項２】　前記鍵生成部は、所定の鍵情報を登録する鍵登録部と、
前記鍵登録部の鍵に基いて前記情報変換手段識別情報を変換して鍵復号鍵を生成する変換部とを具備することを特徴とする請求項１記載のデータコンテンツ利用システム。

【請求項３】　前記データ復号部は、前記鍵復号部の生成した復号鍵に基づいて前記暗号化データコンテンツ及び暗号化コンテンツ識別情報を復号する復号部と、
前記復号部が復号したコンテンツ識別情報とユーザが入力するコンテンツ識別情報とを比較し、双方の識別情報が一致する場合に限り、前記データコンテンツを出力させる比較部とを具備することを特徴とする請求項１記載のデータコンテンツ利用システム。

【請求項４】　前記比較部は、前記双方の識別情報が一致する場合には、前記データコンテンツの一部を出力させると同時に、ユーザが前記データコンテンツの利用を希望するか否かの選択を促すメッセージを出力し、
ユーザが前記データコンテンツの利用を希望すれば前記データコンテンツの全てを出力し、
前記双方の識別情報が不一致の場合には、復号エラーを出力させることを特徴とする請求項３記載のデータコンテンツ利用システム。

【請求項５】　前記情報変換手段あるいは前記利用許可装置には、乱数を出力する乱数発生部を具備し、

2

前記利用許可装置は、情報変換手段識別情報とコンテンツ識別情報と前記乱数発生部が出力する乱数とに基づいて利用許可情報を生成することを特徴とする請求項１記載のデータコンテンツ利用システム。

【請求項６】　前記情報変換手段あるいは前記利用許可装置には、乱数を出力する乱数発生部を具備し、
前記利用許可装置は、コンテンツ識別情報毎にデータコンテンツを復号するための復号鍵を格納する第一の利用権格納部と、
情報変換手段識別情報毎に情報変換手段の認証鍵を格納する第二の利用権格納部とを具備し、
前記利用許可情報生成部は、前記情報変換手段から乱数、コンテンツ識別情報、及び情報変換手段識別情報を受け取ると、前記コンテンツ識別情報で前記第一の利用権格納部を検索して前記コンテンツ識別情報に対応する復号鍵を読み出すと共に、前記情報変換手段識別情報で前記第二の利用権格納部を検索して前記情報変換手段の認証鍵を読み出し、
前記復号鍵を前記認証鍵と前記乱数とに基づいて暗号化することを特徴とする請求項１記載のデータコンテンツ利用システム。

【請求項７】　データコンテンツとこのデータコンテンツを特定するコンテンツ識別情報とを暗号化してなる情報を格納するデータ格納手段と、
個々のデータコンテンツを識別するコンテンツ識別情報毎に利用鍵を登録する利用権格納部と、
ユーザが希望するデータコンテンツを可視的・可聴的なデータとして出力する情報変換手段とを備え、
前記情報変換手段は、ユーザが希望するデータコンテンツを前記データ格納部から読み出すと共に、前記利用権格納部から前記コンテンツ識別情報に対応する利用鍵を読み出す読出部と、
装置固有の装置識別情報に基いて鍵復号鍵を生成する鍵生成部と、
前記鍵生成部の生成した鍵復号鍵及び前記利用鍵に基いて前記暗号化データコンテンツを復号するための復号鍵を生成する鍵復号部と、
前記データコンテンツ読出部が読み出した暗号化データコンテンツを前記鍵復号部が生成した復号鍵に基づいて復号するデータ復号部とを具備することを特徴とするデータコンテンツ利用システム。

【請求項８】　前記鍵生成部は、所定の鍵情報を登録する鍵登録部と、
前記鍵登録部の鍵に基いて前記装置識別情報を変換して鍵復号鍵を生成する変換部とを具備することを特徴とする請求項７記載のデータコンテンツ利用システム。

【請求項９】　前記データ復号部は、前記鍵復号部の生成した復号鍵に基づいて前記暗号化データコンテンツ及び暗号化コンテンツ識別情報を復号する復号部と、
前記復号部が復号したコンテンツ識別情報とユーザが入

力するコンテンツ識別情報とを比較し、双方の識別情報が一致する場合に限り、前記データコンテンツを出力させる比較部とを具備することを特徴とする請求項７記載のデータコンテンツ利用システム。

【請求項１０】　データコンテンツとコンテンツ識別情報とを暗号化してなる情報を格納するデータ格納部と、ユーザが希望するデータコンテンツを可視的・可聴的なデータとして出力する情報変換手段と、

前記データコンテンツの利用許可情報を生成すると共に、データコンテンツの課金情報を管理する利用許可装置とを備え、

前記情報変換手段は、ユーザが希望するデータコンテンツを前記データ格納部から読み出すデータコンテンツ読出部と、

前記情報変換手段を識別する情報変換手段識別情報に基づいて鍵復号鍵を生成する鍵生成部と、

前記鍵生成部の生成した鍵復号鍵及び前記利用許可装置から取得する利用許可情報に基づいて前記暗号化データコンテンツを復号するための復号鍵を生成する鍵復号部と、

前記データコンテンツ読出部が読み出した暗号化データコンテンツを前記鍵復号部が生成した復号鍵に基づいて復号するデータ復号部と、

前記データコンテンツが正常に復号されたか否かを識別する情報を前記利用許可装置へ通知する復号結果通知部とを具備し、

前記利用許可装置は、前記情報変換手段から少なくとも情報変換手段識別情報とコンテンツ識別情報とを受け取り、これらの情報に基いて利用許可情報を生成する利用許可情報生成部と、

前記情報変換手段から復号結果を受けたときに、復号が正常に行われた場合に前記データコンテンツの課金情報を更新する利用量管理部とを具備することを特徴とするデータコンテンツ利用システム。

【請求項１１】　前記鍵生成部は、所定の鍵情報を登録する鍵登録部と、

前記鍵登録部の鍵に基いて前記情報変換手段識別情報を変換して鍵復号鍵を生成する変換部とを具備することを特徴とする請求項１０記載のデータコンテンツ利用システム。

【請求項１２】　前記データ復号部は、前記鍵復号部の生成した復号鍵に基づいて前記暗号化データコンテンツ及び暗号化コンテンツ識別情報を復号する復号部と、

前記復号部が復号したコンテンツ識別情報とユーザが入力するコンテンツ識別情報とを比較し、双方の識別情報が一致するか否かを判別する比較部とを具備することを特徴とする請求項１０記載のデータコンテンツ利用システム。

【請求項１３】　前記情報変換手段あるいは前記利用許可装置には、乱数を出力する乱数発生部を具備し、

前記利用許可装置の利用許可情報生成部は、情報変換手段識別情報とコンテンツ識別情報と前記乱数発生部が出力する乱数とに基づいて利用許可情報を生成することを特徴とする請求項１０記載のデータコンテンツ利用システム。

【請求項１４】　前記利用許可装置は、コンテンツ識別情報毎にデータコンテンツを復号するための復号鍵を登録する第一の利用権格納部と、

情報変換手段識別情報毎に情報変換手段の認証鍵を格納する第二の利用権格納部とを具備し、

前記利用許可情報生成部は、前記情報変換手段からコンテンツ識別情報、及び情報変換手段識別情報を受け取ると、前記コンテンツ識別情報で前記第一の利用権格納部を検索して前記コンテンツ識別情報に対応する復号鍵を読み出すと共に、前記情報変換手段識別情報で前記第二の利用権格納部を検索して前記情報変換手段の認証鍵を読み出し、

前記復号鍵を前記認証鍵に基づいて暗号化して前記情報変換手段へ出力することを特徴とする請求項１０記載のデータコンテンツ利用システム。

【請求項１５】　前記第一の利用権格納部には、コンテンツ識別情報毎にデータコンテンツを復号するための復号鍵と、データコンテンツの課金情報とを格納し、

前記利用量管理部は、前記復号結果通知部から復号結果を受け取ると、前記データコンテンツが正常に復号されたか否かを判別し、正常に復号されていれば前記第一の利用権格納部の課金情報を更新すると共に、

課金情報を正常に更新したか否かを示す情報を前記情報変換手段へ通知することを特徴とする請求項１４記載のデータコンテンツ利用システム。

【請求項１６】　前記情報変換手段は、前記利用許可装置から課金情報を更新したか否かを示す情報を受け取ったときに、この情報と前記比較部の比較結果とを参照し、

前記コンテンツ識別情報が一致し且つ課金情報が正常に更新された場合に、前記データコンテンツを出力し、

前記コンテンツ識別情報が一致し且つ課金情報が正常に更新されなかった場合に、課金エラーを出力し、

前記コンテンツ識別情報が一致しない場合に復号エラーを出力することを特徴とする請求項１５記載のデータコンテンツ利用システム。

【請求項１７】　前記第一の利用権格納部には、コンテンツ識別情報毎にデータコンテンツを復号するための復号鍵と、データコンテンツの課金情報とを格納し、

前記比較部は、前記双方の識別情報が一致する場合には、前記データコンテンツの一部を出力させると同時に、ユーザが前記データコンテンツの利用を希望するか否かの選択を促すメッセージを出力し、

前記復号結果通知部は、前記復号結果とユーザが利用希望か否かを識別する情報とを前記利用量管理部へ通知

し、
前記利用量管理部は、前記復号結果とユーザの利用希望か否かを識別する情報とに基づいて、前記データコンテンツが正常に復号されたか否かを判別すると共にユーザが利用希望か否かを判別し、
前記データコンテンツが正常に復号され且つユーザが利用を希望した場合に限り、前記第一の利用権格納部の課金情報を更新することを特徴とする請求項１４記載のデータコンテンツ利用システム。
【請求項１８】　前記情報変換手段は、前記鍵復号部が復号した復号鍵を保持する復号鍵保持部を備え、
前記復号鍵保持部に前記復号鍵が保持されている間は、前記データ復号部は前記データコンテンツを何回でも復号可能とし、且つ前記利用量管理部は前記第一の利用権格納部の課金情報を更新しないことを特徴とする請求項１０記載のデータコンテンツ利用システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、コンピュータプログラムあるいは映像著作物等のソフトウェア、特にデジタル情報化されたソフトウェアの流通システムに適用して有効な技術に関する。
【０００２】
【従来の技術】ＣＤ－ＲＯＭ等の大規模記憶媒体が出現してくると、この媒体にコンピュータプログラムは勿論、画像や音声をデジタル情報として格納して販売されることが予想される。
【０００３】すなわち、従来ビデオテープで供給されていたような映像著作物がそのままＣＤ－ＲＯＭに格納されて販売されたり、またはＣＤ－ＲＯＭのインタラクティブ性（双方向性）を利用したゲームとして市場に流通し始めてきている。
【０００４】ところで、この種のデジタル情報は他の媒体への複写がきわめて容易であり、且つアナログ情報のような複写による劣化がないことから、同一品質の情報を複製することが可能であり、これらの行為により製造者の利益が害される可能性が極めて高い。すなわち、大容量の書換え可能な光磁気ディスクや磁気ディスク装置さえ所有していればわずかなＤＯＳのコマンドの知識のみでＣＤ－ＲＯＭの内容を複写することが簡単であった。
【０００５】このように十分なセキュリティーチェックが不可能であることを理由にこの種のデジタル情報媒体のレンタル行為は製造者によって禁止されている場合が殆どである。
【０００６】しかしながら、エンドユーザとしては現在のこの種のソフトウェアの価格は高価であり、本当にそのソフトウェアが自身の欲しているものと一致するか、あるいは自身の所有しているハードウェアで使用可能か否かの確認がとれるまでは購入を躊躇する場合が多い。

この点に鑑みて利用が制限されている多数のソフトウェアをＣＤ－ＲＯＭに格納して安価に販売し、エンドユーザはその中から希望のソフトウェアについて代金を支払うことにより、利用制限を解除するためのコードを取得するという新しいソフトウェアの流通方式が実現され始めている。
【０００７】例えば、利用制限の方法として、ソフトウェアを暗号化し、代金の支払いと引き換えに復号の基礎となる許諾情報を取得する方法がある。この方法において、ソフトウェア内にはユーザ個別のユーザ鍵を生成するモジュールと、このユーザ鍵に基づいて許諾情報を復号してソフトウェアの復号鍵を生成し、この復号鍵に基づいてソフトウェアを復号して平文形式のソフトウェアを生成するモジュールを備えている。これにより、代金を支払った正規のユーザは、暗号化されたソフトウェアを復号して利用することができる。
【０００８】
【発明が解決しようとする課題】ところで、上記のシステムでは、正当なユーザが一旦許諾情報を取得すると、この許諾情報を料金を支払っていない他のユーザに提供することにより、データコンテンツを不正に復号して利用してしまう虞がある。
【０００９】また、データコンテンツのレンタルシステムにおいては、ユーザが内容を知らずにレンタルしたデータコンテンツの一部を観賞し、希望のデータと異なっていたために利用を中止しても課金が行われてしまうという問題がある。
【００１０】そこで、本発明は、ソフトウェアの不正利用等を防止し、ソフトウェア利用にかかるセキュリティーの向上を図ると共に、柔軟性のある課金管理を行える技術を提供することを課題とする。
【００１１】
【課題を解決するための手段】本発明は、上記課題を解決するために、以下のような構成を採用した。尚、ここでいうデータコンテンツとは、コンピュータプログラム等の他、映画等の動画像データをはじめとする画像データや音楽等の音声データを含むソフトウェアを示す。
【００１２】＜第一の発明の構成＞第一の発明について図１の原理図に沿って説明する。第一の発明のデータコンテンツ利用システムは、データ格納部３、情報変換手段１、利用許可装置２を備えて構成されている。
【００１３】データ格納部３は、ＣＤ－ＲＯＭ等のようなソフトウェアを格納する媒体、あるいは媒体においてデータを格納する領域を示し、データコンテンツと個々のデータコンテンツを特定するコンテンツ識別情報とを暗号化してなる情報を少なくとも一種類格納している。具体的には、暗号化された情報毎に平文形式のコンテンツ識別情報を格納しており、このコンテンツ識別情報に基づいて各データコンテンツを検索できるようになっている。

【００１４】情報変換手段１は、例えば、データコンテンツを出力する装置に組み込まれるモジュールである。例えば、情報変換手段１は、ビューアとライブラリで構成することができる。この情報変換手段１は、ユーザが希望するデータコンテンツを可視的・可聴的なデータとして出力する機能と、データコンテンツのファイル化を防止する機能と、暗号化された情報を復号する機能とを備えている。ここで、ファイル化を防止する手法として、ビューアにファイル出力ルーチンを持たせない方法がある。

【００１５】一方、利用許可装置２は、例えば、データコンテンツを出力する装置に接続される外部装置であり、各再生装置毎に接続するようにしても良く、あるいは、通信網を介して複数の再生装置で共用するようにしてもよい。そして、利用許可装置２は、データ格納部３に格納されているデータコンテンツの利用許可情報を生成する機能を有している。

【００１６】以下、各構成要素の機能について詳細に説明する。情報変換手段１は、データコンテンツ読出部１ａ、鍵生成部１ｂ、鍵復号部１ｃ、データ復号部１ｄとを具備している。

【００１７】データコンテンツ読出部１ａは、ユーザが希望するデータコンテンツをデータ格納部３から読み出す機能を有している。具体的には、ユーザが入力するコンテンツ識別情報に基づいてデータ格納部３を検索し、暗号化されたデータコンテンツ及びコンテンツ識別情報を読み出す機能を有している。

【００１８】鍵生成部１ｂは、情報変挟手段１を識別する情報変換手段識別情報に基づいて鍵復号鍵を生成するものである。この鍵復号鍵は、暗号化された復号鍵を復号するための暗号解読キー情報であり、復号鍵は暗号化データコンテンツを復号するための暗号解読キー情報である。尚、ここでは、利用許可装置２が生成する利用許可情報が暗号化された復号鍵に相当する。

【００１９】鍵復号部は、鍵生成部の生成した鍵復号鍵で利用許可装置２から取得する利用許可情報を復号し、暗号化データコンテンツを復号するための復号鍵を生成する機能を有している。

【００２０】データ復号部は、データコンテンツ読出部が読み出した暗号化データコンテンツ及び暗号化コンテンツ識別情報とを、鍵復号部が生成した復号鍵に基づいて復号する機能を有している。

【００２１】また、利用許可装置２は、情報変換手段１から少なくとも情報変換手段識別情報とコンテンツ識別情報とを受け取り、これらの情報に基いて利用許可情報を生成する利用許可情報生成部２ａを具備している。

【００２２】上記の構成において、鍵生成部１ｂは、所定の鍵情報を登録する鍵登録部１０と、鍵登録部１０の鍵に基いて情報変換手段識別情報を変換して鍵復号鍵を生成する変換部１１とを備えるようにしてもよい。

【００２３】さらに、データ復号部１ｄは、鍵復号部１ｃの生成した復号鍵に基づいて暗号化データコンテンツ及び暗号化コンテンツ識別情報を復号する復号部１２と、復号されたコンテンツ識別情報とユーザが入力したコンテンツ識別情報とを比較して双方の識別情報が一致する場合に限り復号されたデータコンテンツの出力を許可する比較部１３とを備えるようにしてもよい。

【００２４】また、比較部１３は、復号部１２が復号したコンテンツ識別情報とユーザが入力したコンテンツ識別情報とが一致する場合に、データコンテンツの一部を出力させると共に、このデータコンテンツを参照したユーザに対してデータコンテンツの総てを希望するか否かの選択を促すメッセージを送信する機能を備えるようにしてもよい。そして、比較部１３は、ユーザが上記データコンテンツの全てを希望すれば、全てのデータコンテンツを出力させる。

【００２５】さらに、比較部１３は、復号部１２が復号したデータコンテンツ識別情報とユーザが入力したデータコンテンツ識別情報とが不一致の場合に、復号エラーを出力させる機能をそなえるようにしてもよい。

【００２６】また、上記の構成に加え、情報変換手段１あるいは利用許可装置２に乱数発生部１ｅを備えるようにしてもよい。この乱数発生部１ｅは、任意に乱数を出力するものである。

【００２７】さらに、利用許可装置２は、コンテンツ識別情報毎にデータコンテンツを復号するための復号鍵を格納する第一の利用権格納部２ｂと、情報変換手段識別情報毎に情報変換手段１の認証鍵を格納する第二の利用権格納部２ｃとを具備するようにする。尚、この認証鍵は、鍵復号鍵と同一の情報になるように決定されるものであり、ユーザの不当な取り出しを防止すべく暗号化された状態で格納することが好ましい。そして、利用許可情報生成部２ａは、情報変換手段１から乱数、コンテンツ識別情報、及び情報変換手段識別情報を受け取ると、コンテンツ識別情報で第一の利用権格納部２ｂを検索してコンテンツ識別情報に対応する復号鍵を読み出す機能と、情報変換手段識別情報で第二の利用権格納部２ｃを検索して情報変換手段１の認証鍵を読み出す機能と、認証鍵と乱数とに基づいて復号鍵を暗号化して利用許可情報を生成する機能とを備えるようにする。

【００２８】＜第二の発明の構成＞次に、前記課題を解決する第二の発明について図２の原理図に沿って説明する。

【００２９】第二の発明のデータコンテンツ利用システムは、データ格納部３、利用権格納部４、及び情報変換手段１を備えている。データ格納部３は、暗号化されたデータコンテンツ及び暗号化されたコンテンツ識別情報を格納するものであり、例えばＣＤ－ＲＯＭ、ビデオテープ、カセットテープ等である。

【００３０】利用権格納部４は、個々のデータコンテン

ツを識別するコンテンツ識別情報毎に利用鍵を登録するものである。情報変換手段１は、ユーザが希望するデータコンテンツを可視的・可聴的なデータとして出力する機能を有している。

【００３１】詳細には、情報変換手段１は、データコンテンツ読出部１ａ、鍵生成部１ｂ、鍵復号部１ｃ、及びデータ復号部１ｄを備えている。データコンテンツ読出部１ａは、ユーサが希望するデータコンテンツをデータ格納部３から読み出すと共に、利用権格納部４からコンテンツ識別情報に対応する利用鍵を読み出すものである。

【００３２】鍵生成部１ｂは、ユーザが使用する装置固有の装置識別情報に基いて鍵復号鍵を生成する機能を有している。鍵復号部１ｃは、鍵生成部１ｂが生成した鍵復号鍵と、データコンテンツ読出部１ａが読み出した利用鍵とに従って復号鍵を生成する機能を有している。この復号鍵は、暗号化データコンテンツを復号するための情報である。

【００３３】データ復号部１ｄは、データコンテンツ読出部１ａが読み出した暗号化データコンテンツを鍵復号部１ｃが生成した復号鍵に基づいて復号する機能を有している。

【００３４】さらに、鍵生成部１ｂは、所定の鍵情報を登録する鍵登録部１０と、鍵登録部１０の鍵に基いて装置固有の装置識別情報を変換し、鍵復号鍵を生成する変換部１１とを具備するようにしてもよい。

【００３５】また、データ復号部１ｄは、鍵復号部１ｃの生成した復号鍵に基づいて暗号化データコンテンツ及び暗号化コンテンツ識別情報を復号する復号部１２と、復号部１２が復号したコンテンツ識別情報とユーザが入力するコンテンツ識別情報とを比較し、双方の識別情報が一致する場合に限り、復号部１２が復号したデータコンテンツを出力させる比較部１３とを備えるようにしてもよい。

【００３６】＜第三の発明の構成＞以下に、前記課題を解決する第三の発明について図３の原理図に沿って説明する。

【００３７】第三の発明のデータコンテンツ利用システムは、データ格納部３、情報変換手段１、及び利用許可装置２を備えて構成されている。データ格納部３は、第一、第二の発明と同様であり、説明は省略する。

【００３８】情報変換手投１は、ユーザが希望するデータコンテンツを可視的・可聴的なデータとして出力するものであり、データコンテンツ読出部１ａ、鍵生成部１ｂ、鍵復号部１ｃ、データ復号部１ｄ、及び復号結果通知部１ｇを備えて構成されている。

【００３９】利用許可装置２は、データコンテンツの利用許可情報を生成すると共に、データコンテンツの課金情報を管理するものであり、利用許可情報生成部２ａと利用量管理部２ｄとを備えている。

【００４０】ここで、各構成要素の機能について説明する。データコンテンツ読出部１ａは、ユーザが希望するデータコンテンツをデータ格納部３から読み出す機能を有している。

【００４１】鍵生成部１ｂは、各再生装置に装着された情報変換手段１を識別する情報変換手段識別情報に基づいて鍵復号鍵を生成する機能を有している。鍵復号部１ｃは、鍵生成部１ｂの生成した鍵復号鍵及び利用許可装置２から取得する利用許可情報に基づいて暗号化データコンテンツを復号するための復号鍵を生成する機能を有している。

【００４２】データ復号部１ｄは、データコンテンツ読出部１ａが読み出した暗号化データコンテンツを復号鍵に基づいて復号する機能を有している。復号結果通知部１ｇは、データコンテンツが正常に復号されたか否かを識別する情報を利用許可装置２へ通知する機能を有している。

【００４３】また、利用許可装置２の利用許可情報生成部２ａは、情報変換手段１から少なくとも情報変換手段識別情報とコンテンツ識別情報とを受け取り、これらの情報に基いて利用許可情報を生成する機能を有している。

【００４４】利用量管理部２ｄは、情報変換手段１から復号結果を受けたときに、復号が正常に行われていれば、データコンテンツの課金情報を更新する機能を有している。

【００４５】さらに、上記構成において、鍵生成部１ｂは、所定の鍵情報を登録する鍵登録部１０と、鍵登録部１０の鍵に基いて情報変換手段識別情報を変換して鍵復号鍵を生成する変換部１１とを具備するようにしてもよい。

【００４６】また、データ復号部１ｄは、鍵復号部の生成した復号鍵に基づいて暗号化データコンテンツ及び暗号化コンテンツ識別情報を復号する復号部１２と、復号部１２が復号したコンテンツ識別情報とユーザが入力するコンテンツ識別情報とを比較して双方が一致した場合に、復号部１２が復号したデータコンテンツの出力を許可する機能を有している。

【００４７】さらに、利用許可装置２は、第一の利用権格納部２ｂと第二の利用権格納部２ｃとを備えるようにしてもよい。第一の利用権格納部２ｂは、コンテンツ識別情報毎に各データコンテンツを復号するための復号鍵を登録するものである。第二の利用権格納部２ｃは、情報変換手段識別情報毎に、各情報変換手段が正当な情報変換手段を認証する認証鍵を登録するものである。この認証鍵は、鍵復号鍵と同一の情報となるように決定される情報である。

【００４８】このとき、利用許可情報生成部２ａは、情報変換手段１からコンテンツ識別情報及び情報変換手段識別情報を受信すると、先ずコンテンツ識別情報に基づ

いて第一の利用権格納部２ｂを検索し、前記データコンテンツを復号するための復号鍵を読み出す。次に、利用許可譲歩生成部２ａは、情報変換手段識別情報に基づいて第二の利用権格納部２ｃを検索し、前記情報変換手段１の認証鍵を読み出す機能を有している。さらに、利用許可情報生成部２ａは、復号鍵を認証鍵で暗号化して情報変換手段１へ送信する機能を有している。＊また、第一の利用権格納部２ｂには、コンテンツ識別情報毎にデータコンテンツを復号するための復号鍵に加え、データコンテンツの課金情報とを格納するようにしてもよい。このとき、利用量管理部２ｄは、復号結果通知部１ｇから復号結果を受け取ると、データコンテンツが正常に復号されたか否かを判別する機能と、正常に復号されていれば第一の利用権格納部２ｂの課金情報を更新する機能と、課金情報を正常に更新したか否かを示す情報を情報変換手段１へ通知する機能とを備えるようにする。

【００４９】さらに、情報変換手段１は、利用許可装置２から課金情報を更新したか否かを示す情報を受け取ったときに、この情報と比較部１３の比較結果とに基いて出力すべき情報を判別する機能を有している。すなわち、コンテンツ識別情報が一致し且つ課金情報が正常に更新された場合には、復号されたデータコンテンツを出力させる。また、比較部１３は、コンテンツ識別情報が一致し且つ課金情報が正常に更新されなかった場合には課金エラーを出力させる。コンテンツ識別情報が一致しない場合には復号エラーを出力させる。

【００５０】また、比較部１３は、復号部１２が復号したコンテンツ識別情報と、ユーザが入力したコンテンツ識別情報とが一致する場合に、データコンテンツの一部を出力させると同時に、ユーザがデータコンテンツの利用を希望するか否かの選択を促すメッセージを出力させる機能を備えるようにしてもよい。このとき、復号結果通知部１ｇは、復号結果とユーザが利用希望か否かを識別する情報とを利用量管理部２ｄへ通知する機能を備える。利用量管理部２ｄは、復号結果とユーザの利用希望か否かを識別する情報とを復号して、前記データコンテンツが正常に復号されたか否かを判別すると共にユーザが利用希望か否かを判別する機能を備える。ここで、データコンテンツが正常に復号され且つユーザが利用を希望した場合に限り、利用量管理部２ｄは、第一の利用権格納部２ｂの課金情報を更新するものとする。

【００５１】尚、上記の第三の発明において、情報変換手段１には、鍵復号部１ｃが復号した復号鍵を保持する復号鍵保持部１ｆを備えるようにしてもよい。この場合、復号鍵保持部１ｆに復号鍵が保持されている間は、前記データコンテンツの復号処理を何回でも課金せずに行うことができるようにしてもよい。

【００５２】さらに、情報変換手段１と利用許可装置２とのいずれか一方に、第一の発明と同様に乱数発生部１ｅを備えるようにしてもよい。

【００５３】

【作用】

＜第一の発明の作用＞第一の発明によれば、ユーザが任意のデータコンテンツを利用する場合に、このデータコンテンツのコンテンツ識別情報を入力すると、情報変換手段１のデータコンテンツ読出部１ａは、入力されたコンテンツ識別情報に基づいてデータ格納部３を検索する。そして、データコンテンツ読出部１ａは、データ格納部３から暗号化されたデータコンテンツと暗号化されたコンテンツ識別情報とを読み出す。さらに、データコンテンツ読出部１ａは、暗号化データコンテンツと暗号化コンテンツ識別情報とをデータ復号部１ｄへ通知すると共に、鍵生成部１ｂへ情報変換手段識別情報を通知し、利用許可装置２に対してコンテンツ識別情報と情報変換手段識別情報とを通知する。

【００５４】ここで、利用許可装置２は、情報変換手段１からコンテンツ識別情報と情報変換手投識別情報とを受け取ると、利用許可情報生成部２ａが少なくともコンテンツ識別情報と情報変換手段識別情報とに基づいて利用許可情報を生成する。

【００５５】そして、利用許可装置２は、利用許可情報を情報変換手段１へ送信する。情報変換手段１の鍵生成部１ｂは、情報変換手段識別情報に基づいて鍵復号鍵を生成し、鍵復号部１ｃへ通知する。

【００５６】鍵復号部１ｃは、鍵生成部１ｂが生成した鍵復号鍵を、利用許可装置２から受け取った利用許可情報で復号して復号鍵を生成する。次に、情報変換手段１のデータ復号部１ｄは、鍵復号部１ｃが復号した復号鍵に基づいて暗号化データコンテンツと暗号化コンテンツ識別情報とを復号する。詳細には、データ復号部１ｄの復号部１２が暗号化データコンテンツと暗号化コンテンツ識別情報とを復号し、復号したコンテンツ識別情報を比較部１３へ通知する。

【００５７】比較部１３は、復号部１２が復号したコンテンツ識別情報と、ユーザが入力したコンテンツ識別情報とを比較し、双力が一致した場合に限り復号したデータコンテンツを出力させる。

【００５８】尚、比較部１３は、双方のコンテンツ識別情報が一致した場合に、復号されたデータコンテンツの一部を出力させると共に、このデータコンテンツの利用をユーザが希望するか否かを選択させるメッセージを出力させるようにしてもよい。この場合、ユーザが上記メッセージに応答してデータコンテンツの利用を希望すれば、比較部１３は、復号したデータコンテンツをすべて出力させる。また、比較部１３は、双方のコンテンツ識別情報が一致した場合に、復号されたデータコンテンツを一定時間出力させると共に、このデータコンテンツの利用をユーザが希望するか否かを選択させるメッセージを出力させるようにしてもよい。この場合、ユーザが一定時間内にデータコンテンツの利用を希望すれば、比較

部１３は、一定時間経過後も引続きデータコンテンツを出力させる。一方、ユーザがデータコンテンツの利用を希望しない場合、あるいはユーザが一定時間内に応答しない場合には、比較部１３は、一定時間経過後にデータコンテンツの出力を停止させる。

【００５９】また、比較部１３は、双方のコンテンツ識別情報が不一致の場合、あるいはコンテンツ識別情報が正常に復号されなかった場合には、復号エラーを示すメッセージを出力させる。

【００６０】ここで、情報変換手段１に乱数発生部１ｅを備え、利用許可装置２が第一の利用権格納部２ｂ及び第二の利用権格納部２ｃを備えた場合には、情報変換手段１は、乱数発生部１ｅから出力される乱数と自身の情報変換手段識別情報とユーザが入力したコンテンツａ識別情報とを利用許可装置２へ送信する。

【００６１】利用許可装置２の利用許可情報生成部２ａは、先ずコンテンツ識別情報に基づいて第一の利用権格納部２ｂを検索し、暗号化データコンテンツの復号鍵を読み出す。次に、利用許可情報生成部２ａは、情報変換手段識別情報に基づいて第二の利用権格納部２ｃを検索し、情報変換手段１の認証鍵を読み出す。

【００６２】さらに、利用許可情報生成部２ａは、認証鍵と乱数とに基づいて復号鍵を暗号化し、情報変換手段１へ送信する。情報変換手段１の鍵復号部１ｃは、利用許可装置２から暗号化された復号鍵を受信すると、この暗号化復号鍵を鍵生成部１ｂが生成した鍵復号鍵で復号し、データ復号部１ｄへ通知する。

【００６３】データ復号部１ｂは、鍵復号部１ｃが復号した復号鍵で、暗号化データコンテンツを復号する。このとき、データ復号部１ｂの比較部１３は、復号部１２が復号したコンテンツ識別情報とユーザが入力したコンテンツ識別情報とを比較し、双方が一致すれば復号したデータコンテンツの出力を許可する。一方、双方のコンテンツ識別情報が不一致の場合には、比較部１３は、復号エラーを示すメッセージを出力させる。

【００６４】＜第二の発明の作用＞第二の発明によれば、ユーザが希望のデータコンテンツのコンテンツ識別情報を入力した時に、情報変換手段１のデータコンテンツ読出部１ａは、コンテンツ識別情報に基づいてデータ格納部３を検索し、コンテンツ識別情報に対応する暗号化データコンテンツと暗号化コンテンツ識別情報とを読み出す。これと同時に、データコンテンツ読出部１ａは、コンテンツ識別情報に基づいて利用権格納部４を検索し、前記コンテンツ識別情報に対応する利用鍵情報を読み出す。

【００６５】そして、鍵生成部１ｂの変換部１１は、鍵登録部１０から所定の鍵情報を読み出し、この鍵情報に基づいて鍵復号鍵を生成する。次に、鍵復号部１ｃは、鍵生成部１ｂが生成した鍵復号鍵と、データコンテンツ読出部１ａが読み出した利用鍵とに基づいて復号鍵を生成し、この復号鍵をデータ復号部１ｄへ通知する。

【００６６】データ復号部１ｄは、鍵復号部１ｃが生成した復号鍵に基づいて、データコンテンツ読出部１ａが読み出した暗号化データコンテンツを復号し、出力する。詳細には、データ復号部１ｄの復号部１２が鍵復号部１ｃで復号された復号鍵に基づいてデータコンテンツ読出部１ａが読み出した暗号化データコンテンツと暗号化コンテンツ識別情報とを復号する。そして、比較部１３が復号部１２が復号したコンテンツ識別情報とユーザが入力したコンテンツ識別情報とを比較し、双方のコンテンツ識別情報が一致すると、復号されたデータコンテンツを出力させる。一方、双方のコンテンツ識別情報が不一致の場合、例えばコンテンツ識別情報の復号が正常に行われなかった場合に、比較部１３は、復号のエラーを示すメッセージを出力させる。

【００６７】また、比較部１３は、双方のコンテンツ識別情報が一致した場合には、復号部１２が復号したデータコンテンツの一部を出力させると同時に、ユーザに対してデータコンテンツを利用するか否かの選択を促すメッセージを出力させるようにしても良い。そして、ユーザが上記データコンテンツの利用を希望すれば、比較部１３は、復号したデータコンテンツのすべてを出力する。

【００６８】＜第三の発明の作用＞第三の発明によれば、ユーザが希望のデータコンテンツのコンテンツ識別情報を入力したときに、データコンテンツ読出部１ａは、ユーザが入力したコンテンツ識別情報に基づいてデータ格納部３を検索し、暗号化データコンテンツ及び暗号化コンテンツ識別情報とを読み出す。そして、データ読出部１ａは、ユーザが入力したコンテンツ識別情報と自身の情報変換手段識別情報とを利用許可装置２へ送信すると共に、情報変換手段識別情報を鍵生成部１ｂへ通知し、暗号化データコンテンツ及び暗号化コンテンツ識別情報をデータ復号部１ｄへ通知する。

【００６９】また、鍵生成部１ｂの変換部１１は鍵登録部１０から所定の鍵情報を読み出し、この鍵情報と情報変換手段識別情報とに基づいて鍵復号鍵を生成する。一方、利用許可装置２の利用許可情報生成部２ａは、情報変換手段１から受信したコンテンツ識別情報に基づいて第一の利用権格納部２ｂを検索し、暗号化データコンテンツを復号する復号鍵を読み出すと共に、情報変換手段識別情報に基づいて第二の利用権格納部２ｃを検索し、情報変換手段の認証鍵を読み出す。そして、利用許可情報生成部２ａは、復号鍵を認証鍵で暗号化して情報変換手段１へ送信する。

【００７０】このとき、情報変換手段１の鍵復号部１ｃは、利用許可装置２から受信した暗号化復号鍵を鍵復号鍵で復号し、データ復号部１ｄへ通知する。データ復号部１ｄの復号部１２は、データコンテンツ読出部１ａが読み出した暗号化データコンテンツと暗号化コンテンツ

識別情報とを復号鍵で復号し、復号したコンテンツ識別情報を比較部１３へ通知する。

【００７１】比較部１３は、復号部１２が復号したコンテンツ識別情報とユーザが入力したコンテンツ識別情報とを比較し、双方が一致するか否かを判別し、復号が正常に終了したか否かを復号結果通知部１ｇへ通知する。

【００７２】復号結果通知部１ｇは、比較部１３から受け取った復号結果を利用許可装置２へ送信する。利用許可装置２の利用量管理部２ｄは、情報変換手段１から受信した復号結果を参照し、復号が正常に終了していれば、第一の利用権格納部２ｂに格納されているデータコンテンツの課金情報を更新する。一方、利用量管理部２ｄは、復号が正常に行われていなければ、第一の利用権格納部２ｂに格納されているデータコンテンツの課金情報は更新しない。

【００７３】さらに、利用量管理部２ｄは、課金情報が正常に更新できたか否かを示す課金結果を情報変換手段１へ送信する。情報変換手段１は、利用許可装置２から受信した課金結果を参照して課金が正常に行われたか否か判別すると共に、比較部１３の復号結果を参照して復号が正常に終了したか否かを判別する。

【００７４】ここで、情報変換手段１は、課金が正常に行われ且つ復号が正常に行われていれば、復号したデータコンテンツを出力する。また、情報変換手段１は、課金あるいは復号の少なくとも一方が正常に行われなかった場合には、エラーを示す情報を出力する。詳細には、情報変換手段１は、コンテンツ識別情報が一致し且つ課金情報が正常に更新されなかった場合に、課金エラーを出力し、コンテンツ識別情報が一致しない場合に復号エラーを出力する。尚、比較部１３は、データコンテンツを出力させるときに、復号部１２が復号したデータコンテンツの一部を出力させると同時に、ユーザがデータコンテンツの利用を希望するか否かの選択を促すメッセージを出力するようにしてもよい。これに対応して復号結果通知部１ｇは、利用許可装置２へ復号結果と共にユーザが利用希望か否かを識別する情報を送信するようにする。

【００７５】また、利用許可装置２の利用量管理部２ｄは、復号結果とユーザの利用希望か否かを識別する情報とに基づいて、データコンテンツが正常に復号されたか否かを判別すると共にユーザが利用希望か否かを判別する。ここで、利用量管理部２ｄは、データコンテンツが正常に復号され且つユーザが利用を希望した場合に限り、第一の利用権格納部２ｂの課金情報を更新する。

【００７６】さらに、

【００７７】

【実施例】以下、本発明の実施例について図面に沿って説明する。

＜実施例１＞実施例１におけるデータコンテンツ利用システムを適用するパーソナルコンピュータのハードウェア構成を図４に示す。

【００７８】本実施例１では、データコンテンツを格納するデータ格納手段として、ＣＤ－ＲＯＭ等の記憶媒体３を例に挙げて説明する。このＣＤ－ＲＯＭには、データコンテンツとこのデータコンテンツのコンテンツＩＤとからなる情報を暗号化された状態で格納している。この暗号化情報は、少なくとも一種類格納されており、各情報は平文形式のコンテンツ識別情報毎に格納されている。

【００７９】尚、データコンテンツの販売元にデータコンテンツを格納すると共に、この販売元と各ユーザのパーソナルコンピュータとを通信回線で接続し、通信回線によりデータコンテンツを提供するようにしてもよい。

【００８０】データコンテンツ利用制御システムは、記憶媒体３からデータを読み出すドライバ装置を備えたパーソナルコンピュータ４０に、利用許可装置２を接続して構成されている。ユーザは、データコンテンツを購入する際に、このデータコンテンツを復号する鍵情報を利用許可装置２に登録してもらう。この鍵情報は、セキュリティを確保するために暗号化された状態で登録するものとする。

【００８１】そして、利用許可装置２は、データコンテンツの販売元が暗号化した復号鍵情報を登録し、パーソナルコンピュータ４０には、ユーザが希望のデータコンテンツのコンテンツＩＤを入力するためのキーボード７、画像データを出力するディスプレイ装置５、及び音声データを出力するスピーカ６が接続されている。

【００８２】以下に、本実施例１におけるパーソナルコンピュータ４０と利用許可装置５の機能について説明する。

（パーソナルコンピュータ４０の機能）図５は、パーソナルコンピュータ４０の機能構成を示すブロック図である。

【００８３】この機能は、メモリに格納された制御プログラムをｃＰＵが実行することにより実現される機能である。本実施例１では、パーソナルコンピュータ４０は、ビューア１００とライブラリ１１０とを備えている。

【００８４】ビューア１００は、任意のデータコンテンツを可視的・可聴的な情報として、ディスプレイ装置５あるいはスピーカ６から出力させる機能を有している。ライブラリ１１０は、利用許可装置２の許可を受けると、暗号化されたデータコンテンツ（以下、暗号化データコンテンツと記す）を復号化する機能を有している。

【００８５】（ビューア１００の機能）ビューア１００の機能別構成を図６に示す。このビューア１００は、データをファイル化するルーチンを持たないモジュールであり、データ読出部１００ａ、及びデータ出力部１００ｂを備えている。

【００８６】データ読出部１００ａは、キーボード７か

らコンテンツＩＤが入力されると、このコンテンツＩＤに基づいて記憶媒体３へアクセスし、暗号化データコンテンツと暗号化されたコンテンツＩＤ（以下、暗号化コンテンツＩＤと記す）とを読み出す。さらにデータ読出部１００ａは、コンテンツＩＤと暗号化データコンテンツと暗号化コンテンツＩＤとに加え、自ビューアを特定するビューアＩＤとをライブラリ１１０へ通知する機能を有している。

【００８７】一方、データ出力部１００ｂは、ライブラリ１１０で復号されたデータコンテンツをディスプレイ装置５あるいはスピーカ６から出力させる機能を有している。詳細には、ライブラリ１１０において正常に復号化されたデータコンテンツのみを出力する。

【００８８】（ライブラリ１１０の機能）ライブラリ１１０の機能について図７に沿って説明する。ライブラリ１１０は、鍵生成部１１０ｂ、鍵復号部１１０ｃ、データ復号部１１０ｄ、及び乱数発生部１１０ｅを備えている。

【００８９】鍵生成部１１０ｂは、自ライブラリを特定するライブラリ鍵を登録する鍵登録部１０と、ビューア１００から受け取ったビューアＩＤを鍵登録部１０のライブラリ鍵で変換して鍵復号鍵を生成する変換部１１とを備えている。

【００９０】鍵復号部１１０ｂは、利用許可装置２から利用許可情報として暗号化された復号鍵を受信し、この暗号化復号鍵を鍵生成部１１０ｂが生成した鍵復号鍵で復号する機能を有している。

【００９１】データ復号部１１０ｄは、ビューア１００から受け取った暗号化データコンテンツと暗号化コンテンツＩＤとを鍵復号部１１０ｃが復号した復号鍵で復号する機能を有している。詳細には、データ復号部１１０ｄは、復号鍵で暗号化データコンテンツと暗号化コンテンツＩＤとを復号する復号部１２を備えている。さらに、データ復号部１２は、復号部１２が復号したコンテンツＩＤとユーザが入力したコンテンツＩＤとを比較して、復号処理が正常に行われたか否かを判別し、この判別結果をビューア１００へ通知する比較部１３を備えている。

【００９２】これに対して、ビューア１００のデータ出力部１００ｂは、比較部１３の判別結果に基づいて復号部１２が復号したデータコンテンツを出力させるか否かを決定する。つまり、データ出力部１００ｂは、復号処理が正常に行われた場合に限り、データコンテンツを出力する。一方、データコンテンツの復号処理が正常に行われなかった場合には、比較部１３は、ビューア１００から復号エラーを示すメッセージを出力させる。

【００９３】（利用許可装置２の機能）図８は、本実施例１における利用許可装置２の機能別構成ブロック図である。同図に示す機能は、利用許可装置２の備えるプロセッサが、メモリに格納された制御プログラムを実行することにより実現される機能である。

【００９４】利用許可装置２は、利用許可情報生成部２ａ、第一の利用権格納部２ｂ、及び第二の利用権格納部２ｃを備えている。第一の利用権格納部２ｂは、コンテンツＩＤ毎に、各暗号化データコンテンツを復号する復号鍵を登録するものである。

【００９５】第二の利用権格納部２ｃは、ビューアＩＤ毎に、各ビューアの認証鍵を登録するものである。尚、この認証鍵は、鍵復号鍵と等しくなるように決定される情報である。

【００９６】利用許可情報生成部２ａは、本発明の利用許可情報としての復号鍵情報を生成する機能を有している。具体的には、利用許可情報生成部２ａは、ライブラリ１１０から受信したコンテンツＩＤに基づいて第一の利用権格納部２ｂを検索してデータコンテンツの復号鍵を検出する機能と、ライブラリ１１０から受信したビューアＩＤに基づいて第二の利用権格納部２ｃを検索してビューアの認証鍵を検出する機能と、復号鍵情報を認証鍵情報で暗号化する機能とを備えている。

【００９７】次に、本実施例１におけるパーソナルコンピュータ４０と利用許可装置２の動作について説明する。

（パーソナルコンピュータ４０の動作）先ず、図９に沿ってビューア１００の動作について説明する。

【００９８】パーソナルコンピュータ４０のユーザがキーボード７から希望のデータコンテンツのコンテンツＩＤを入力すると（ステップ９０１）、ビューア１００のデータ読出部１００ａは、このコンテンツＩＤに基づいて記憶媒体３へアクセスし、暗号化データコンテンツと暗号化コンテンツＩＤとを読み出す（ステップ９０２）。

【００９９】そして、データ読出部１００ａは、暗号化データコンテンツ、暗号化コンテンツＩＤ、ユーザが入力したコンテンツＩＤ、及びビューアＩＤをライブラリ１１０へ通知する（ステップ９０３）。

【０１００】このとき、ライブラリ１１０では、暗号化データコンテンツと暗号化コンテンツＩＤの復号処理を行う。さらに、ライブラリ１１０は、復号したコンテンツＩＤとユーザが入力したコンテンツＩＤとを比較して、両者が一致したか否かを判別する情報をビューア１００へ通知する。ビューア１００は、比較結果を受け取ると（ステップ９０４）、この比較結果に基づいて復号処理が正常に終了したか否かを認識する（ステップ９０５）。

【０１０１】ここで、復号処理が正常に終了していれば、データ出力部１００ｂは、復号部１２が復号したデータコンテンツをディスプレイ装置５あるいはスピーカ６から出力させる（ステップ９０６）。

【０１０２】上記ステップ９０５に於て、復号処理が正常に終了していなければ、データ出力部１００ｂは、復

号エラーを示すメッセージをディスプレイ装置5あるいはスピーカ6から出力させる（ステップ907）。

【0103】次に、図10に沿ってライブラリ110の動作について説明する。ライブラリ110は、ビューア100からビューアID、暗号化データコンテンツ、暗号化コンテンツID、及びユーザが入力したコンテンツIDを受け取ると（ステップ1001）、コンテンツIDとビューアIDと乱数発生部110eの生成した乱数を利用許可装置へ送信する（ステップ1002）。さらに、ライブラリ110は、ビューアIDを鍵生成部110bへ通知し、暗号化データコンテンツ及び暗号化コンテンツIDをデータ復号部110dへ通知する。

【0104】そして、鍵生成部110bの変換部11は、ビューアIDを鍵登録部10のライブラリ鍵で変換し鍵復号鍵情報を生成する（ステップ1003）。また、利用許可装置2から暗号化された復号鍵情報を受け取ると（ステップ1004）、鍵復号部110cは、この暗号化復号鍵を鍵復号鍵で復号する（ステップ1005）。

【0105】データ復号部110bの復号部12は、暗号化データコンテンツと暗号化コンテンツIDとを復号鍵で復号する（ステップ1006）。ここで、比較部13は、復号部12が復号したコンテンツIDとユーザが入力したコンテンツIDとを比較して（ステップ1007）、双方のコンテンツIDが一致するか否かを判別する（ステップ1008）。

【0106】ここで、双方のコンテンツIDが一致した場合、すなわち復号化が正常に終了した場合には、比較部13は、復号化が正常に終了した旨と共に復号したデータコンテンツをビューア100へ通知する（ステップ1009）。

【0107】上記ステップ1008において、双方のコンテンツIDが不一致の場合、すなわち、復号処理が正常に終了しなかった場合には、比較部13は、比較結果のみをビューア100へ通知する（ステップ1010）。

【0108】（利用許可装置2の動作）利用許可装置2の動作について図11のフローチャート図に沿って説明する。利用許可装置2の利用許可情報生成部2aは、ライブラリ110からコンテンツID、ビューアID、及び乱数を受信すると（ステップ1101）、コンテンツIDに基づいて第一の利用権格納部2bを検索する。そして、利用許可情報生成部2aは、第一の利用権格納部2bから上記データコンテンツの復号鍵情報を読み出す（ステップ1102）。

【0109】さらに、利用許可情報生成部2aは、ビューアIDに基づいて第二の利用権格納部2cを検索し、上記ビューア100の認証鍵情報を読み出す（ステップ1103）。ここで、利用許可情報生成部2aは、復号鍵情報を、認証鍵情報と乱数とに基づいて暗号化し（ステップ1104）、この暗号化復号鍵情報をライブラリ110へ送信する（ステップ1105）。

【0110】（実施例1の効果）実施例1によれば、データコンテンツを出力する専用ビューアを設けることにより、データのファイル化を防止することができる。

【0111】さらに、復号鍵情報をビューア毎の認証鍵とライブラリで発生した乱数とで暗号化することにより、ユーザの解読行為を防止し、データコンテンツの不正利用を防止することができる。

【0112】＜実施例2＞本実施例2におけるデータコンテンツ利用システムを適用するソフトウェア再生装置14のハードウェア構成を図12に示す。

【0113】本実施例2は、CD－ROM3に格納されたデータコンテンツを販売する流通形態の実施例である。同図に示すソフトウェア再生装置14は、CD－ROMに格納されたデータコンテンツを再生・出力する装置である。

【0114】なお、本実施例では説明の便宜のため、暗号化データコンテンツをCD－ROMに格納して提供されたものとするが、通信情報として得られたものであってもよい。

【0115】（ソフトウエア再生装置14の構成）このソフトウェア再生装置14は、共通のデータフォーマットによって提供されたこれら各種データコンテンツを、統一的に取り扱うことができる情報機器である。具体的には、これら各種データコンテンツを読み込み、コンピュータプログラムの実行，映画プログラム及びテレビジョンプログラムの再生（画像信号の再生，音声信号の再生），音楽データの再生（音声信号の再生），静止画の表示等を行う機能を有している。なお、映画プログラム及びテレビジョンプログラムにおいては、画像信号と音声信号は、互いに同期して出力されるように関連付けられている。　そして、ソフトウェア再生装置14は、CD－ROMに対して、図示せぬドライブ装置により読み出しが行われる。この図示せぬドライブ装置によって読み出されたデータフレームは、復調回路・制御回路15に入力される。この復調回路・制御回路15は、入力されたデータフレームのうち、MPEG規格の画像・音声情報を、復調してデコーダ16に送信する機能を有している。

【0116】デコーダ16は、エラー訂正及びビットの並び替えを実行して最大2メガバイト／秒（平均1メガバイト／秒）の画像・音声情報を、SD回路19に引き渡す機能を有している。デコーダ16は、この画像・音声情報の引き渡しを行うために、I／O（入出力）装置19aを介して、SD回路19内のシステムバスBに接続されている。

【0117】このSD回路19内のシステムバスBには、I／O装置19aを介して、インタフェース装置17も接続されている。このインタフェース装置17は、

このソフトウェア再生装置１４の外面に設けられている図示しない操作キー，フロッピーディスクドライブ装置，及びモデムとＳＤ回路１９との間の入出力処理を行う。そして、通信網を介して送信されるデータコンテンツが、この図示せぬモデム装置，及びインタフェース装置１７によってＳＤ回路１９に入力される。この通信によって供給されるデータコンテンツも、ＣＤ－ＲＯＭにより供給されるデータコンテンツと同様の形式を有しており、予め暗号化（及び圧縮処理）されている。

【０１１８】次に、これらデコーダ１５及びインタフェース１７に接続されるＳＤ回路１９の機能について説明する。

（ＳＤ回路の機能及び構成）ソフトウェア再生装置１４に提供される各種データコンテンツは、上述のＣＤ－ＲＯＭや通信の様に、入手が容易な形態で流通されるので、その使用許諾を如何にするかが問題となる。そのため用いられるのがＳＤ回路１９である。即ち、このソフトウェア再生装置１４で再生可能な各種データコンテンツは、暗号化された状態で流通される。この暗号化された各種データコンテンツは、ＳＤ回路１９によって、逐次復号化される。

【０１１９】なお、このＳＤ回路１９は、ソフトウェア再生装置１４のカードスロット（たとえばＰＣＭＣＩＡ準拠のカードスロット）内に着脱自在に装着されたＩＣカードの形態で実現される。

【０１２０】さらに、ＳＤ回路１９は、バスＢに対して相互に接続された制御ＣＰＵ１９ｃ，ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）１９ｄ，メモリ１９ｅ，並びにＩ／Ｏ装置１９ａ及び１９ｂから構成されている。

【０１２１】制御ＣＰＵ１９ｃは、ソフトウェア再生装置１４内のホスト制御ｃＰＵ１８と分担して、デコーダ１５及びデマルチプレクサ２０とＤＥＳ１９ｄとの間での情報のやりとりを制御する。また、制御ＣＰＵ１９ｃは、ＤＥＳ１９ｄの制御を行う機能も有している。

【０１２２】メモリ１９ｅには、制御ＣＰＵ１９ｃの制御プログラムを格納している。ＤＥＳ１９ｄは、デコーダ１６から受け取った画像・音声情報を復号化する機能と、データコンテンツの運用によって生じたユーザ情報を暗号化する機能を有する。なお、このユーザ情報は、インタフェース１７を介して接続されている図示せぬモデムにより、通信網を通ってデータコンテンツの権利者に通知されるか、若しくは、フロッピーディスクＦＤに書き込まれて、データコンテンツの権利者によって回収される。

【０１２３】ＤＥＳ１９ｄにより復号化されたデータ（画像データ，音声データ等）フレームは、Ｉ／Ｏ装置１９ｂを通じて、ＳＤ回路１９外のデマルチプレクサ２０に送出される。デマルチプレクサ２０は、音声データフレーム，画像データフレーム，並びにコンピュータプログラム及びそのデータを分離する。そして、画像データフレームをＭＰＥＧ伸長回路（ＭＰＥＧ－２）２１に出力し、音声データフレームをＭＰＥＧ伸長回路（ＭＰＥＧ－２）２２に出力し、コンピュータプログラム及びそのデータをＭＰＥＧ伸長回路（ＭＰＥＧ－２）２３に出力する。

【０１２４】ＭＰＥＧ伸長回路（ＭＰＥＧ－２）２１、２２、２３は、ＭＰＥＧ規格で圧縮されたままの状態で送信されて来た画像データフレーム，又は音声データフレームを伸長して、画像又は音声出力可能なフォーマットに復元する回路である。これらＭＰＥＧ伸長回路（ＭＰＥＧ－２）２１、２２、２３においてデータフレームの伸長をする際には、ＶＲＣ回路２４によって出力の同期がとられる。即ち、ＶＲＣ回路２４から出力される同期信号に同期して、ＭＰＥＧ伸長回路（ＭＰＥＧ－２）２１、２２、２３は、伸長されたデータフレームを出力するのである。なお、ＭＰＥＧ伸長回路としては、１Ｃチップ「ＩＳＯ／ＩＢＣ　ＣＤ　１３８１８’１～３」を用いることができる。

【０１２５】そして、画像用のＭＰＥＯ伸長回路（ＭＰＥＧ－２）２１からの出力は、Ｄ／Ａ変換器（ＤＡ）２５によってアナログ信号に変換される。このアナログ信号は、ソフトウェア再生装置１４に接続されている図示せぬＴＶモニタ装置に向けて出力される。また、音声用のＭＰＥＧ伸長回路（ＭＰＥＧ－２）２２からの出力は、Ｄ／Ａ変換器（ＤＡ）２６によってアナログ信号に変換される。このアナログ信号は、そのまま、ソフトウェア再生装置１４に接続されている図示せぬスピーカに向けて出力される。一方、コンピュータ用のプログラム又はデータは、ＭＰＥＧ伸長回路（ＭＰＥＧ－２）２３をそのまま通過してソフトウェア再生装置１４に接続されている図示せぬコンピュータに向けて出力される。

【０１２６】ここで、本発明のデータコンテンツ利用システムを実現すべき機能及び構成について説明する。

（データコンテンツ利用システムの構成）本発明のデータコンテンツ利用システムは、ソフトウェア再生装置１４の制御ＣＰＵ１８が図示しないメモリに登録された制御プログラムを実行することにより実現される。

【０１２７】ここで、実施例２におけるデータコンテンツ利用制御システムの機能別構成を図１３に示す。同図においてデータコンテンツ利用制御システムは、ビューア１００及びライブラリ１１０と、利用権格納部４と、データ格納部としてのＣＤ－ＲＯＭ３とを備えている。

【０１２８】ＣＤ－ＲＯＭ３は、実施例１と同様に、データコンテンツとコンテンツＩＤとからなる情報を暗号化して格納しており、この情報は平文形式のコンテンツＩＤ毎に登録されている。

【０１２９】利用権格納部４は、メモリ１９ｅ上に設けられており、コンテンツＩＤ毎に、各データコンテンツの利用鍵情報を格納している。そして、ユーザは、デー

タコンテンツを購入する際に、購入元へＳＤ回路１９を持参し、この利用権格納部４にデータコンテンツの復号情報を書き込んでもらう。この復号情報は、セキュリティ確保のために暗号化された状態で書き込まれている。

【０１３０】ビューア１００は、ユーザが希望するデータコンテンツを可視的・可聴的な情報としてＴＶモニタ、スピーカ、あるいはパーソナルコンピュータＰＣから出力させる機能を有している。

【０１３１】ライブラリ１１０は、暗号化データコンテンツを復号する機能を有している。以下に、ビューア１００とライブラリ１１０の機能について詳細に説明する。

（ビューアの機能）実施例２のビューア１００の機能構成は、前述の実施例１と同様であり、データ読出部１００ａとデータ出力部１００ｂとを備えている。

【０１３２】データ読出部１００ａは、ソフトウェア再生装置１４の外面に設けられている操作キーからユーサが入力するコンテンツＩＤをインタフェース１７，Ｉ／Ｏ装置１９ａ，及びバスＢを介して受け、このコンテンツＩＤに基づいＣＤ－ＲＯＭに格納されている暗号化データコンテンツ及び暗号化コンテンツＩＤを復調回路・制御回路１５、デコーダ１６、Ｉ／Ｏ１９ａ、及びシステムバスＢを介して読み出す機能を有している。

【０１３３】さらに、本実施例２のデータ読出部１００ａは、コンテンツＩＤに基づいて利用権格納部４を検索し、データコンテンツの利用鍵情報を読み出す機能を有している。この利用鍵情報は、暗号化データコンテンツを復号する復号鍵情報を暗号化した情報である。

【０１３４】データ出力部１００ｂは、ライブラリ１１０で復号されたデータコンテンツを可視的・可聴的なデータとして、Ｉ／Ｏ１９ｂ，デマルチプレクサ２０、ＭＰＥＧ伸長回路（ＭＰＥＧ－２）２１・２２・２３、及びＤ／Ａ変換器（ＤＡ）２５・２６を介してＴＶモニタ、スピーカ、あるいはパーソナルコンピュータＰＣから出力させる機能を有している。

【０１３５】（ライブラリ１１０の機能）実施例２におけるライブラリ１１０の機能別構成を図１４に示す。同図において、実施例２のライブラリ１１０は、鍵生成部１１０ｂ、鍵復号部１１０ｃ、及びデータ復号部１１０ｄを備えている。

【０１３６】鍵生成部１１０ｂは、自ライブラリ１１０固有のライブラリ鍵を保持する鍵登録部１０と、制御ＣＰＵ１８を特定するＣＰＵ－ＩＤを鍵登録部１０のライブラリ鍵で変換して鍵復号鍵を生成する変換部１１とを備えている。

【０１３７】鍵復号部１１０ｃは、ビューア１００が読み出した利用鍵情報を鍵復号鍵で復号して、復号鍵を生成する機能を有している。データ復号部１１０ｄは、ビューア１００が読み出した暗号化データコンテンツを鍵復号部１１０ｃが復号した復号鍵で復号化する機能を有している。詳細には、データ復号部１１０ｄは、復号部１２と比較部１３とを備えている。復号部１２は、ビューア１００が読み出した暗号化データコンテンツ及び暗号化コンテンツＩＤを、鍵復号部１１０ｃが生成した復号鍵で復号する機能を有している。一方、比較部１３は、復号部１２が復号したコンテンツＩＤとユーザが入力したコンテンツＩＤとを比較して双方が一致するか否か、すなわち復号処理が正常に終了したか否かを判別する機能を有している。さらに、比較部１３は、双方のコンテンツＩＤが一致すると、ビューア１００へ復号したデータコンテンツの出力を許可する機能も有している。

【０１３８】以下、本実施例２におけるデータコンテンツ利用制御システムの動作について説明する。

（データコンテンツ利用制御システムの動作）先ず、ビューア１００の動作について図１５に沿って説明する。

【０１３９】ビューア１００のデータ読出部１００ａは、ユーザが操作キーにより希望のデータコンテンツのコンテンツＩＤを入力すると（ステップ１５０１）、このコンテンツＩＤに基づいてＣＤ－ＲＯＭ３を検索して暗号化データコンテンツと暗号化コンテンツＩＤとを読み出す（ステップ１５０２）。これと同時に、データ読出部１００ａは、コンテンツＩＤに基づいて利用権格納部４を検索し、上記データコンテンツの利用鍵情報を読み出す（ステップ１５０３）。

【０１４０】そして、データ読出部１００ａは、暗号化データコンテンツ、暗号化コンテンツＩＤ、利用鍵情報、及びユーザが入力したコンテンツＩＤをライブラリ１１０へ通知する（ステップ１５０４）。このとき、ライブラリ１１０では、暗号化データ及び暗号化コンテンツＩＤの復号処理を行い、復号したコンテンツＩＤとユーザが入力したコンテンツＩＤとを比較した結果をビューア１００へ通知する。

【０１４１】そして、データ出力部１００ｂは、ライブラリ１１０の比較部１３から比較結果を通知されると（ステップ１５０５）、データコンテンツの復号処理が正常に終了したか否かを認識する（ステップ１５０６）。

【０１４２】ここで、データコンテンツの復号処理が正常に終了していれば、データ出力部１００ｂは、ライブラリ１１０が復号したデータコンテンツをＴＶモニタ、スピーカ、あるいはパーソナルコンピュータＰＣから出力する（ステップ１５０７）。

【０１４３】上記ステップ１５０６において、ライブラリから復号処理が正常に終了しなかった旨を通知されると、データ出力部１００ｂは、復号エラーを示すメッセージをＴＶモニタ、スピーカ、あるいはパーソナルコンピュータＰＣから出力する（ステップ１５０８）。

【０１４４】次に、ライブラリ１１０の動作について図１６に沿って説明する。ライブラリ１１０では、ビューア１００からコンテンツＩＤ、暗号化データコンテン

ツ、暗号化コンテンツＩＤ、及び利用権情報を受け取った時に（ステップ１６０１）、鍵生成部１１０ｂの変換部１１が制御ＣＰＵ１９ｃのＣＰＵ－ＩＤを、鍵登録部１０のライブラリ鍵で変換して鍵復号鍵を生成し、これを鍵復号部１１０ｃへ通知する（ステップ１６０２）。

【０１４５】鍵復号部１１０ｃは、ビューア１００から受け取った利用権情報を、鍵生成部１１０ｂが生成した鍵復号鍵で復号して復号鍵を生成する（ステップ１６０３）。

【０１４６】そして、データ復号部１１０ｄの復号部１２は、鍵復号部１１０ｃが生成した復号鍵に基づいて暗号化データコンテンツと暗号化コンテンツＩＤとを復号する（ステップ１６０４）。このとき、比較部１３は、復号部１２が復号したコンテンツＩＤとユーザが入力したコンテンツＩＤとを比較し（ステップ１６０５）、双力が一致するか否かを判別する（ステップ１６０６）。

【０１４７】ここで、双方のコンテンツＩＤが一致すれば、復号処理が正常に終了した旨を示す情報とデータコンテンツとをビューア１００へ通知する（ステップ１６０７）　上記ステップ１６０６において、双方のコンテンツＩＤが一致しない場合、すなわち復号処理が正常に終了しなかった場合には、比較部１３は、その旨を示す比較結果のみをビューア１００へ通知する（ステップ１６０８）。

【０１４８】（実施例２の効果）実施例２によれば、データコンテンツを復号する復号鍵を、ソフトウェア再生装置固伯のＣＰＵ－ＩＤとライブラリ鍵とに基づいて暗号化することにより、ユーザがライブラリ及びＳＤ回路を使用せずに、復号鍵を取り出すのを防止することができる。これにより、復号鍵を購入してないユーザが不正にデータコンテンツを利用することを防止することができる。

【０１４９】＜実施例３＞実施例３におけるデータコンテンツ利用システムは、前述の実施例１と同様にパーソナルコンピュータに利用許可装置２を接続したシステムを例に挙げて説明する。

【０１５０】また、本実施例３のデータコンテンツ利用システムは、データコンテンツをユーザに貸し出し、ユーザが利用した量に応じて課金を行うシステムを例に挙げて説明する。

【０１５１】図１７に本実施例３における利用許可装置２の機能別構成を示す。本実施例３における利用許可装置２は、利用許可情報生成部２ａ、第一の利用権格納部２ｂ、及び第二の利用権格納部２ｃに加え、利用量管理部２ｄを備えている。

【０１５２】また、第一の利用権格納部２ｂには、コンテンツＩＤ毎に、各データコンテンツの復号鍵情報に加え、課金情報が格納されている。この課金情報は、各データコンテンツ毎に格納されており、ユーザが利用する度に減算されるポイント情報としている。つまり、課金情報は、ユーザが記憶媒体３から読み出した暗号化データコンテンツを復号すると減算される。そして、ユーザは、データコンテンツをレンタル業者へ返却する際に、利用許可装置２を持参し、業者がこの課金情報を解読することにより精算を行う。また、利用許可装置２とレンタル業者とを通信回線等で接続し、課金情報のみを業者側へ送信するようにしてもよい。

【０１５３】利用量管理部２ｄは、第一の利用権格納部２ｂに格納されている課金情報を管理するものであり、データコンテンツの復号処理が正常に終了し、ユーザがデータコンテンツの利用を希望した場合に限り、そのデータコンテンツの課金ポイントを”１”減算する機能を有している。さらに、利用量管理部２ｄは、課金情報の更新が正常に行われると、すなわち、減算後の課金ポイントが”０”以上であれば、課金処理終了通知をライブラリ２へ送信する機能を有している。

【０１５４】（ライブラリ１１０の機能）実施例３におけるライブラリ１１０の機能別構成を図１８に示す。同図において、ライブラリ１１０は、鍵生成部１１０ｂ、鍵復号部１１０ｃ、データ復号部１１０ｄ、復号鍵保持部１１０ｆ、及び復号結果通知部１１０ｇを備えている。

【０１５５】鍵生成部１１０ｂは、白ライブラリ１１０を特定するライブラリ鍵を登録する鍵登録部１０、及びビューアＩＤをライブラリ鍵で変換して鍵復号鍵を生成する変換部１１を備えている。

【０１５６】鍵復号部１１０ｃは、利用許可装置２から受信した暗号化復号鍵を、鍵生成部１１０ｂが生成した鍵復号鍵で復号する機能を有している。データ復号部１１０ｄは、暗号化データコンテンツと暗号化コンテンツＩＤとを鍵復号部１１０ｃが復号した復号鍵情報で復号する復号部１２、及び復号部１２が復号したコンテンツＩＤとコーザが入力したコンテンツＩＤとを比較して復号処理が正常に終了したか否かを判別する比較部１３を備えている。比較部１３は、復号処理が正常に終了した場合（コンテンツＩＤが一致する場合）には、復号部１２が復号したデータコンテンツの一部とユーザがデータコンテンツの利用を希望するか否かの選択を促すメッセージをビューア１００へ通知する機能を有している。また、比較部１３は、復号処理が正常に終了しなかった場合には復号処理結果のみをビューア１００へ通知する機能も有している。

【０１５７】復号鍵保持部１１０ｆは、鍵復号部１１０ｃが復号した復号鍵情報を登録するものであり、データ復号部１１０ｄは復号鍵保持部１１０ｆに復号鍵情報が保持されている限りはこの復号鍵情報に基づいて上記データコンテンツを何回でも復号可能としている。

【０１５８】復号結果通知部１１０ｇは、復号処理が正常に終了し、且つユーザがデータコンテンツの利用を希望する場合に、復号結果を利用許可装置２へ通知し、課

金処理を要求する機能を有している。これに対して、利用許可装置2の利用量管理部2dは、第一の利用権格納部2bにおける前記データコンテンツの課金ポイントを”1”減算するものとする。

【0159】そして、利用許可装置2から課金処理結果を受信したときに、復号結果通知部110gは、この課金処理結果をビューア100へ通知する機能を有している。さらに、比較部13は、課金処理が正常に終了した旨を認識すると、復号したデータコンテンツの全てをビューア100へ通知する。

【0160】尚、復号結果通知部110gは、データ復号部110dが復号鍵保持部110fの復号鍵に基づいてデータコンテンツを復号化した場合には、この復号結果を利用許可装置2へ通知しないものとする。すなわち、利用許可装置2は、復号鍵保持部110fの復号鍵に基づいて何回復号処理を行っても課金ポイントを減算しないようにしている。

【0161】その他の構成及び機能は、前述の実施例1と同様であり、説明は省略する。以下、本実施例3におけるデータコンテンツ利用制御システムの動作について図面に沿って説明する。

【0162】（パーソナルコンピュータ40の動作）パーソナルコンピュータ40の動作として先ずビューア100の動作について図19に沿って説明する。

【0163】ユーザがキーボード7から希望のデータコンテンツのコンテンツIDを入力すると（ステップ1901）、ビューア100のデータ読出部100aは、コンテンツIDに基づいて記憶媒体3を検索して暗号化データコンテンツと暗号化コンテンツIDとを読み出す（ステップ1902）。

【0164】そして、データ読出部100aは、暗号化データコンテンツ、暗号化コンテンツID、ビューアID、及びユーザが入力したコンテンツIDをライブラリ110へ通知する（ステップ1903）。

【0165】そして、データ出力部100bは、ライブラリ110から復号処理結果を受け取る（ステップ1904）。ここで、復号処理が正常に終了していれば、データ出力部100bは、ライブラリ110が復号したデータコンテンツの一部と、ユーザがデータコンテンツの利用を希望するか否かの選択を促すメッセージとをディスプレイ装置5あるいはスピーカ6から出力する（ステップ1905、ステップ1906）。

【0166】ここで、ビューア100は、ユーザがデータコンテンツの利用を希望すれば、この旨をライブラリ110へ通知する（ステップ1908）。そして、ビューア100のデータ出力部100bは、ライブラリ110から前記データコンテンツの課金処理が正常に終了した旨の通知を受けると（ステップ1909）、ライブラリ110が復号したデータコンテンツの全てをディスプレイ装置5あるいはスピーカ6から出力する（ステップ1910）。

【0167】また、上記ステップ1905において、復号処理が正常に終了しなかった場合には、データ出力部100bは、復号エラーを示すメッセージをディスプレイ装置5あるいはスピーカ6から出力する（ステップ1911）。

【0168】上記ステップ1909において、課金処理が正常に終了しなかった場合には、データ出力部100bは、課金エラーを示すメッセージをディスプレイ装置5あるいはスピーカ6から出力する（ステップ1912）。

【0169】次に、ライブラリ110の動作について図20に沿って説明する。ライブラリ110は、ビューア100からコンテンツID、ビューアID、暗号化データコンテンツ、及び暗号化コンテンツIDを受け取ると（ステップ2001）、コンテンツIDとビューアIDとを利用許可装置2へ送信する（ステップ2002）。

【0170】鍵生成部110bの変換部11は、鍵登録部10のライブラリ鍵に基づいてビューアIDを変換し、鍵復号鍵情報を生成する（ステップ2003）。そして、利用許可装置2から暗号化復号鍵情報を受信すると（ステップ2004）、鍵復号部110cは、暗号化復号鍵を鍵生成部110bが生成した鍵復号鍵で復号する（ステップ2005）。

【0171】データ復号部110cの復号部12は、鍵復号部110cが復号した復号鍵で暗号化データコンテンツ及び暗号化コンテンツIDを復号する（ステップ2006）。

【0172】ここで、比較部13は、復号部12が復号したコンテンツIDとユーザが入力したコンテンツIDとを比較し（ステップ2007）、復号処理が正常に終了したか否かを判別する（ステップ2008）。そして、比較部13は、復号処理が正常に終了していれば、データコンテンツの一部とユーザがデータコンテンツの利用を希望するか否かの選択を促すメッセージをビューア100へ通知する（ステップ2009）。

【0173】そして、ビューア100から、上記メッセージに対してユーザが希望する旨の通知を受け取ると（ステップ2010）、復号結果通知部110gは、復号処理が正常に終了した旨を利用許可装置2へ送信する（ステップ2011）。

【0174】ここで、利用許可装置2が上記データコンテンツの課金処理を行い、その結果を送信してくると（ステップ2012）、復号結果通知110gは、この課金処理結果を比較部13へ通知すると同時に、ビューア100へ通知する。

【0175】比較部13は、課金処理が正常に終了していれば（ステップ2013）、復号したデータコンテンツの全てをビューア100へ通知する（ステップ2014）。

【０１７６】ステップ２００８において、復号処理が正常に終了していなければ、比較部１３が復号結果のみをビューア１００へ通知する（ステップ２０１５）。ステップ２０１３において、課金処理が正常に終了していなければ、復号結果通知部１１０ｇが課金処理結果をビューア１００へ通知し、比較部１３は、何も送信しない（ステップ２０１６）。

【０１７７】（利用許可装置２の動作）本実施例３における利用許可装置２の動作について図２１に沿って説明する。利用許可装置２の利用許可情報生成部２ａは、ライブラリ１１０からコンテンツＩＤ及びビューアＩＤを受信すると（ステップ２１０１）、コンテンツＩＤに基づいて第一の利用権格納部２ｂを検索する。そして、利用許可情報生成部２ａは、第一の利用権格納部２ｂから上記データコンテンツの復号鍵情報を読み出す（ステップ２１０２）。

【０１７８】さらに、利用許可情報生成部２ａは、ビューアＩＤに基づいて第二の利用権格納部２ｃを検索し、上記ビューア１００の認証鍵情報を読み出す（ステップ２１０３）。ここで、利用許可情報生成部２ａは、復号鍵情報を認証鍵情報に基づいて暗号化し（ステップ２１０４）、この暗号化復号鍵情報をライブラリ１１０へ送信する（ステップ２１０５）。

【０１７９】その後、ライブラリ１１０から復号結果通知を受け取ると（ステップ２１０６）、利用量管理部２ｄは、この通知から復号処理が正常に終了したか否かを判別する（ステップ２１０７）。

【０１８０】ここで、復号処理が正常に終了していれば、利用量管理部２ｄは、コンテンツＩＤに基づいて第一の利用権格納部２ｂへアクセスし、上記データコンテンツの課金ポイントを”１”デクリメントする（ステップ２１０８）。そして、利用量管理部２ｄは、減算後の課金ポイントが負数であるか否かを判別して、課金処理が正常に終了したか否かを判別する（ステップ２１０９）。

【０１８１】そして、利用量管理部２ｄは、課金処理が正常に終了していれば、この旨をライブラリ１１０へ通知する（ステップ２１１０）。一方、課金処理が正常に終了しなかった場合には、この旨をライブラリ１１０へ通知する（ステップ２１１１）。

【０１８２】（実施例３の効果）実施例３によれば、データコンテンツを出力する専用ビューアを設けることにより、データのファイル化を防止することができる。

【０１８３】さらに、復号鍵情報をビューア毎の認証鍵とライブラリ固有のライブラリ鍵とで暗号化することにより、ユーザの解読行為を防止し、データコンテンツの不正利用を防止することができる。

【０１８４】また、本実施例３では、復号鍵を保持しておき、この復号鍵が保持されている間は、何回でも復号化を行える。さらに、本実施例３のシステムによれば、データコンテンツのレンタル行為に対する課金をおこなえるだけでなく、ユーザに対して復号されたデータコンテンツの一部を提供し、ユーザが本当に希望するデータコンテンツであれば課金をおこなうことにより、サービス性が向上する。

【０１８５】尚、上記の実施例３において、ライブラリ１１０と利用許可装置２との間で送受信される課金情報等は、暗号化して送受信するようにしてもよい。

【０１８６】

【発明の効果】本発明によれば、ソフトウェアの不正利用等を防止し、ソフトウェア利用にかかるセキュリティーの向上を図ると共に、安全で柔軟な課金管理を行うことができる。

【図面の簡単な説明】

【図１】第一の発明の原理図

【図２】第二の発明の原理図

【図３】第三の発明の原理図

【図４】実施例１におけるパーソナルコンピュータのハードウェア構成図

【図５】実施例１におけるパーソナルコンピュータの機能別構成ブロック図

【図６】実施例１におけるビューアの機能別構成ブロック図

【図７】実施例１におけるライブラリの機能別構成ブロック図

【図８】実施例１における利用許可装置の機能別構成ブロック図

【図９】実施例１におけるビューアの動作フローチャート図

【図１０】実施例１におけるライブラリの動作フローチャート図

【図１１】実施例１におけろ利用許可装置の動作フローチャート図

【図１２】実施例２におけるデータコンテンツ利用制御システムを適用するソフトウェア再生装置のハードウェア構成図

【図１３】実施例２におけるデータコンテンツ利用制御システムの機能別構成ブロック図

【図１４】実施例２におけるライブラリの機能別構成ブロック図

【図１５】実施例２におけるビューアの動作フローチャート図

【図１６】実施例２におけるライブラリの動作フローチャート図

【図１７】実施例３における利用許可装置の機能別構成ブロック図

【図１８】実施例３におけるライブラリの機能別構成ブロック図

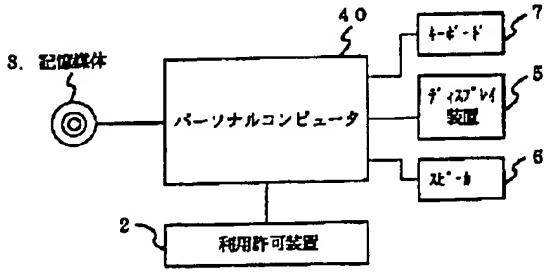
【図１９】実施例３におけるビューアの動作フローチャート図

31　　32

【図２０】実施例３におけるライブラリの動作フローチャート図
【図２１】実施例３における利用許可装置の動作フローチャート図
【符号の説明】
１・・情報変換手段
１ａ・・データコンテンツ読出部
１ｂ・・鍵生成部
１ｃ・・鍵復号部
１ｄ・・データ復号部
１ｅ・・乱数発生部
１ｆ・・復号鍵保持部
１ｇ・・復号結果通知部
２・・利用許可装置
２ａ・・利用許可情報生成部
２ｂ・・第一の利用権格納部
２ｃ・・第二の利用権格納部
２ｄ・・利用量管理部
３・・データ格納部（記憶媒体、ＣＤ－ＲＯＭ）
４・・利用権格納部
５・・ディスプレイ装置
６・・スピーカ
７・・キーボード
１０・・鍵登録部
１１・・変換部
１２・・復号部
１３・・比較部
１４・・ソフトウェア再生装置
１５・・復調回路
１６・・デコーダ
１７・・インターフェース
１８・・制御ＣＰＵ
１９・・ＳＤ回路
１９ａ・・Ｉ／Ｏ
１９ｂ・・Ｉ／Ｏ
１９ｃ・・制御ＣＰＵ
１９ｄ・・ＤＥＳ
１９ｅ・・メモリ
２０・・デマルチプレクサ
２１・・ＭＰＥＧ伸長回路
２２・・ＭＰＥ　　Ｇ伸長回路
２３・・ＭＰＥＧ伸長回路
２４・・ＶＲＣ回路
２５・・Ｄ／Ａ変換器
２６・・Ｄ／Ａ変換器
４０・・パーソナルコンピュータ
１００・・ビューア
１００ａ・・データ読出部
１００ｂ・・データ出力部
１１０・・ライブラリ
１１０ｂ・・鍵生成部
１１０ｃ・・鍵復号部
１１０ｄ・・データ復号部
１１０ｅ・・乱数発生部
１１０ｆ・・復号鍵保持部
１１０ｇ・・復号結果通知部

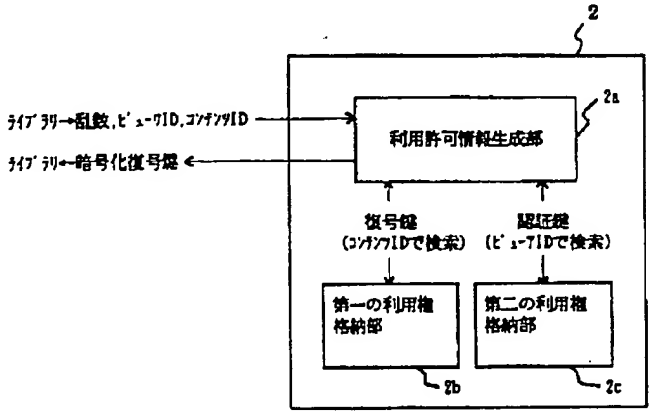
【図４】

実施例１におけるパーソナルコンピュータのハードウェア構成図

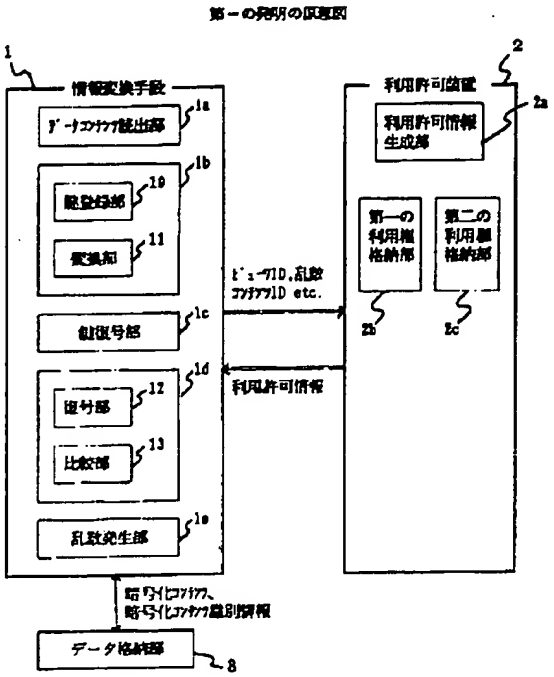


【図８】

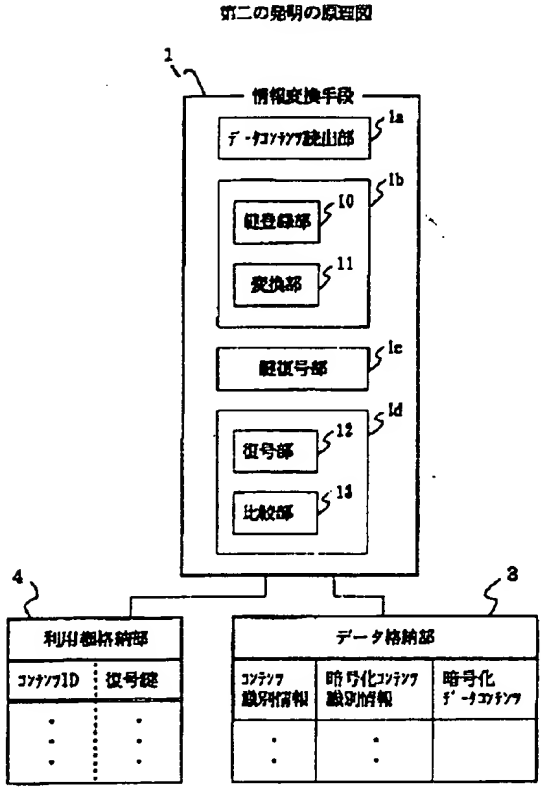
実施例１における利用許可装置の機能別構成ブロック図



【図１】

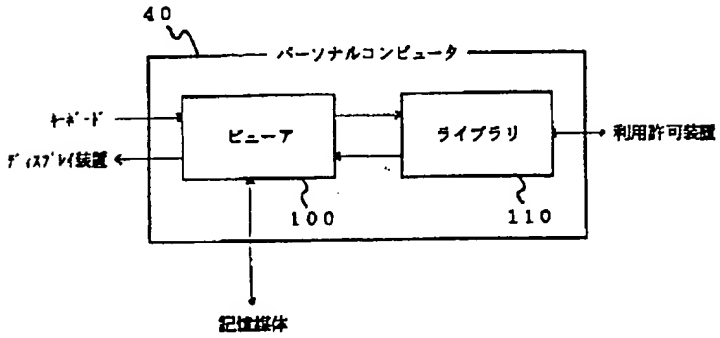


【図２】



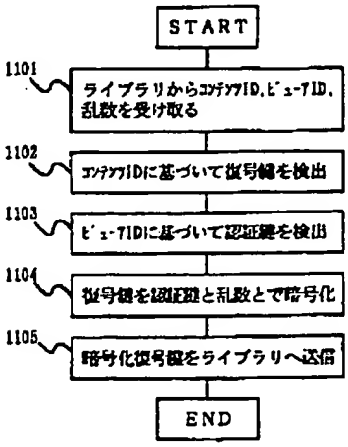
【図５】

実施例１におけるパーソナルコンピュータの機能別構成ブロック図



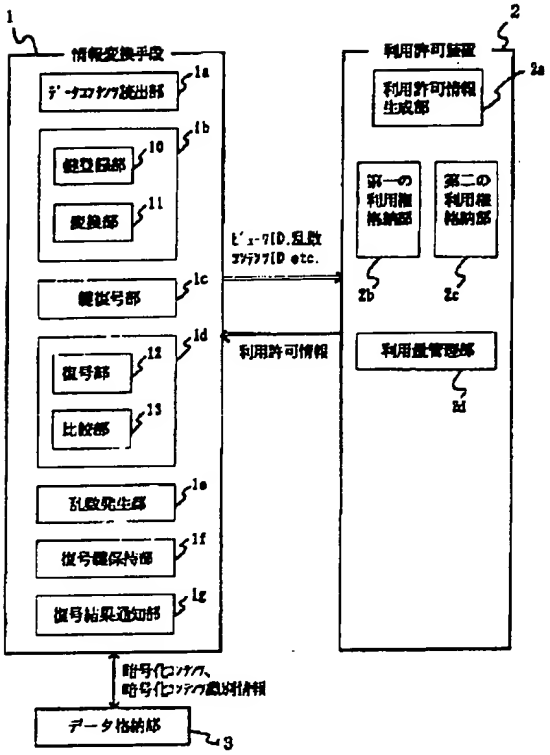
【図１１】

実施例１における利用許可装置の動作フローチャート図



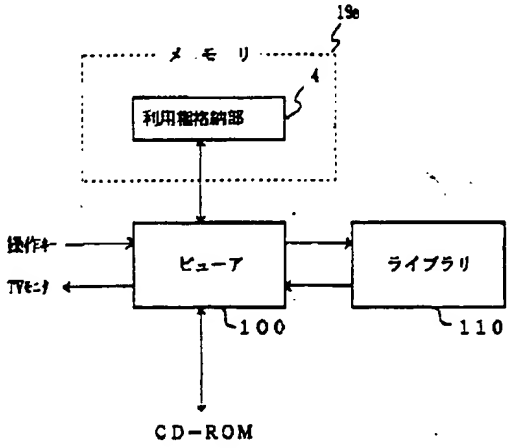
【図３】

第三の発明の原理図



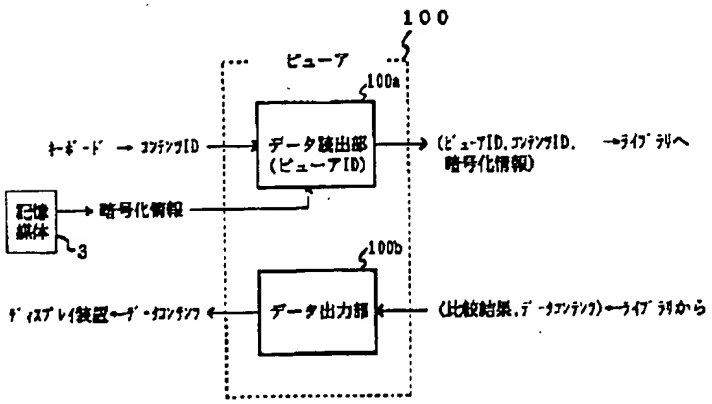
【図１３】

実施例２におけるデータコンテンツ利用制御システムの機能別構成ブロック図



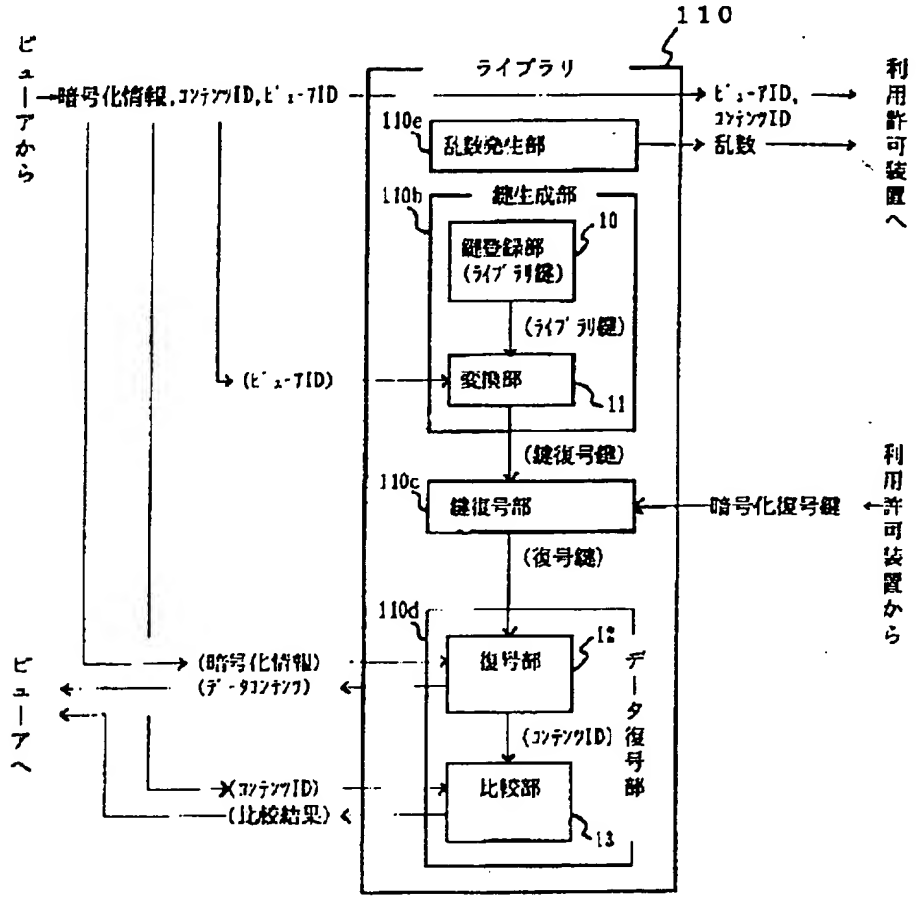
【図６】

実施例１におけるビューアの機能別構成ブロック図



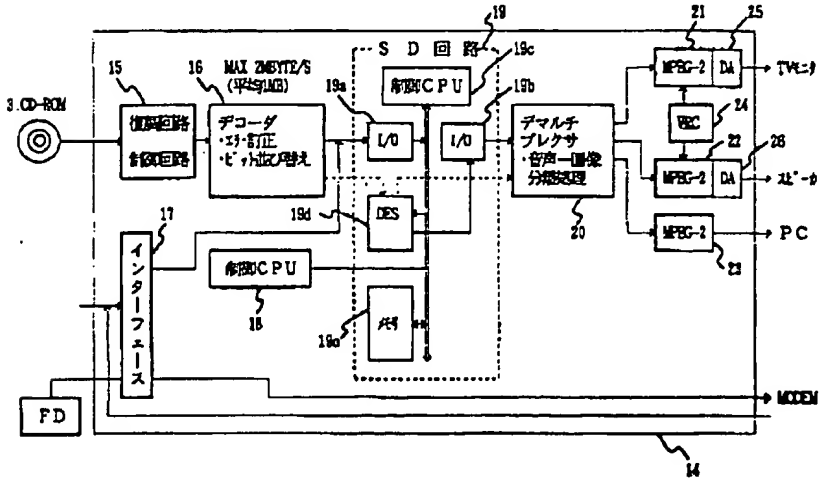
【図７】

実施例１におけるライブラリの機能別構成ブロック図



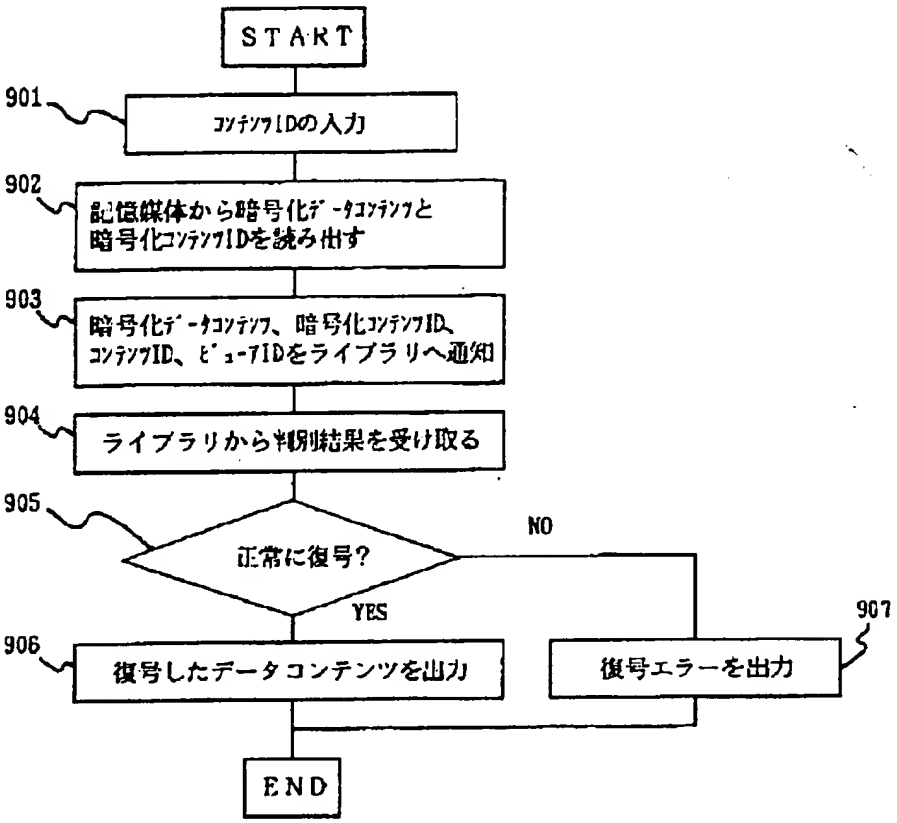
【図１２】

実施例２におけるデータコンテンツ不正使用制御システムを適用するソフトウェア再生装置のハードウェア構成図



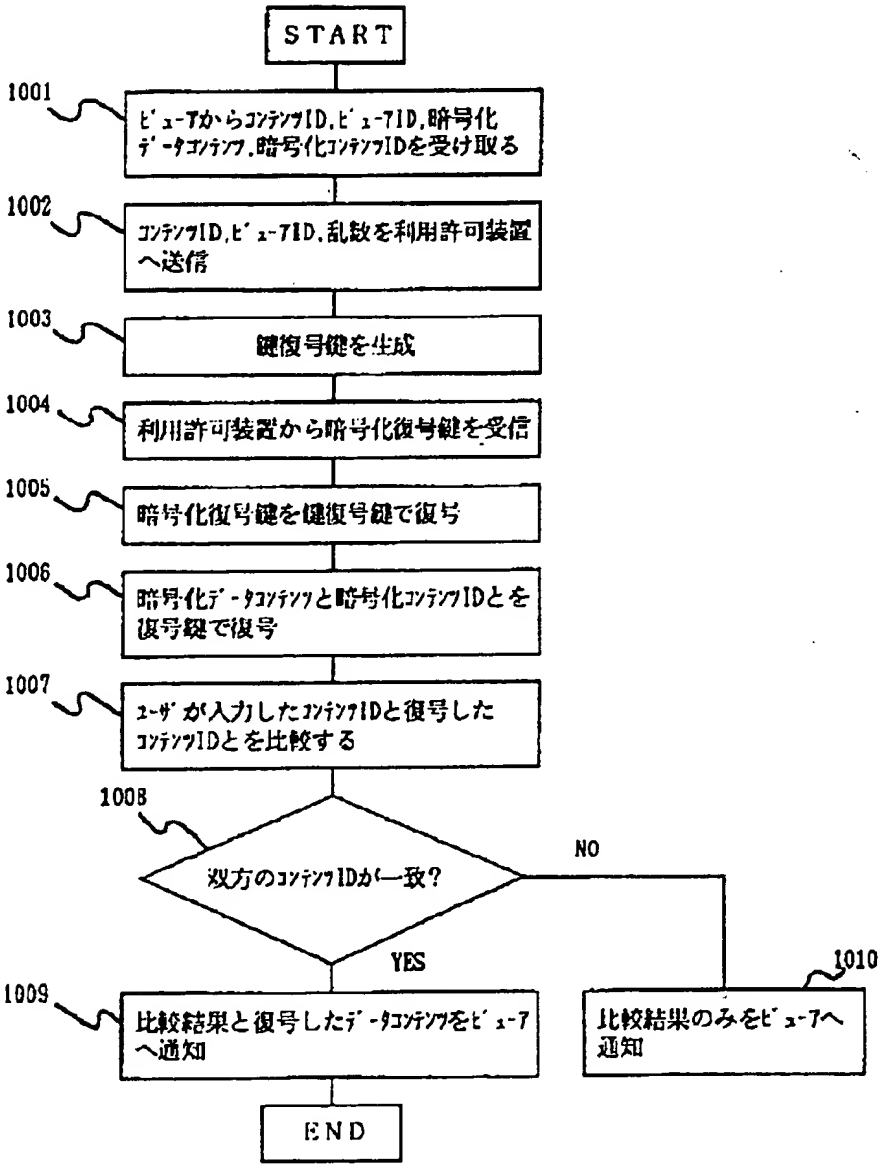
【図９】

実施例１におけるビューアの動作フローチャート図



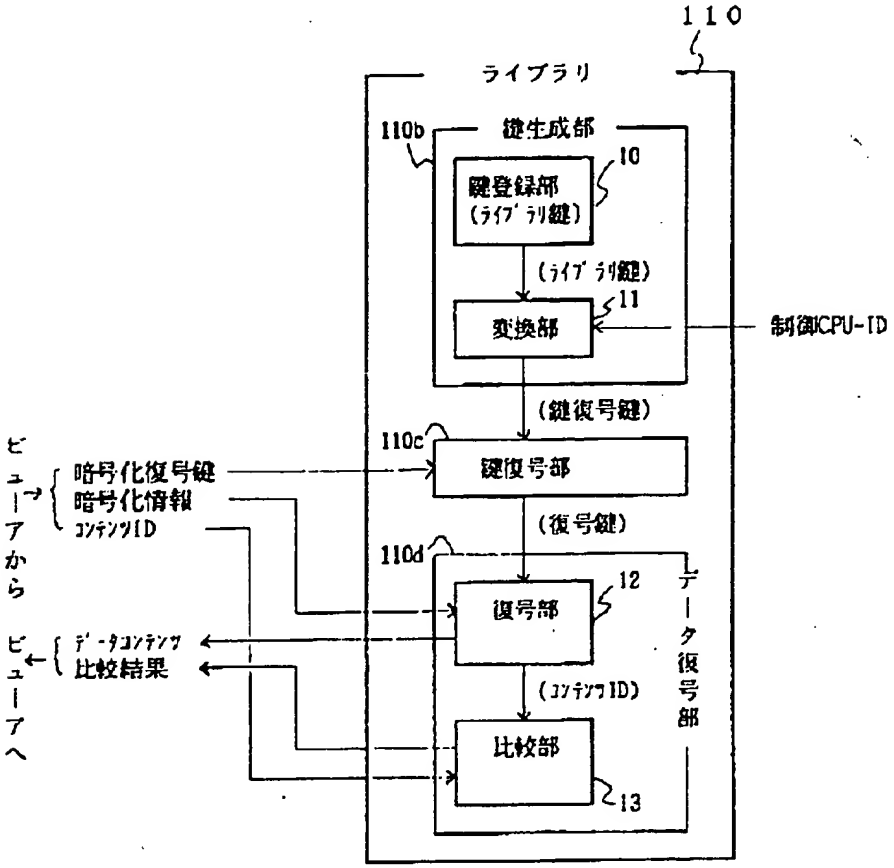
【図１０】

実施例１におけるライブラリの動作フローチャート図



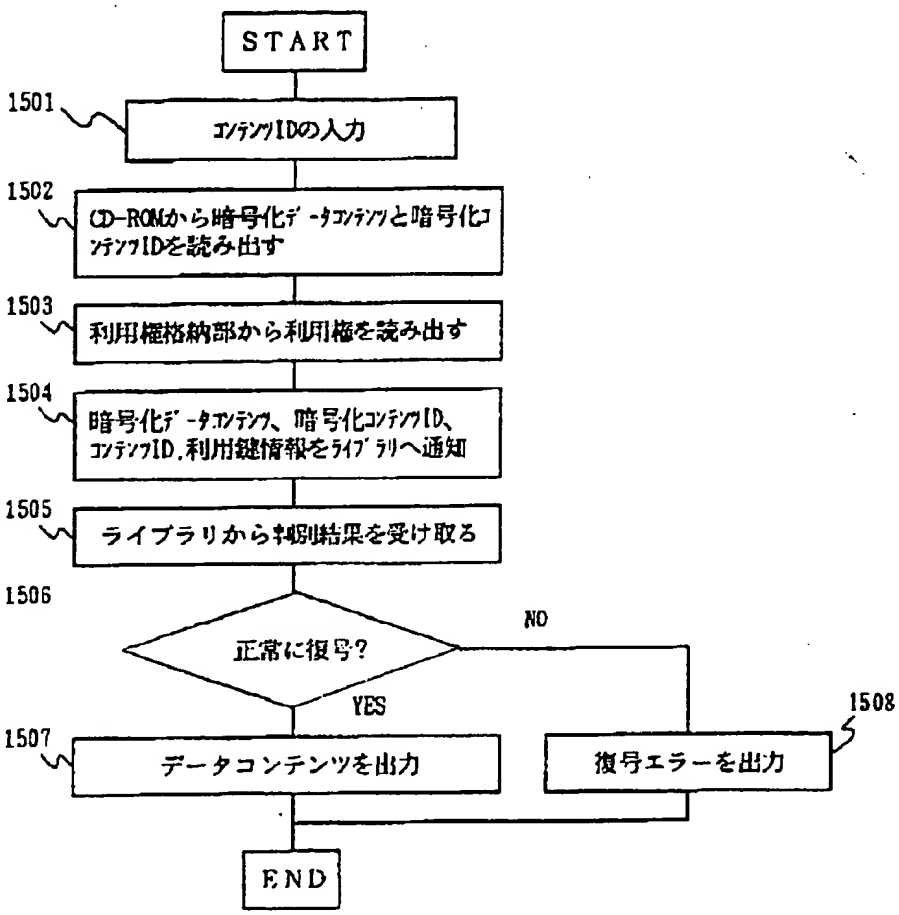
【図１４】

実施例２におけるライブラリの機能別構成ブロック図



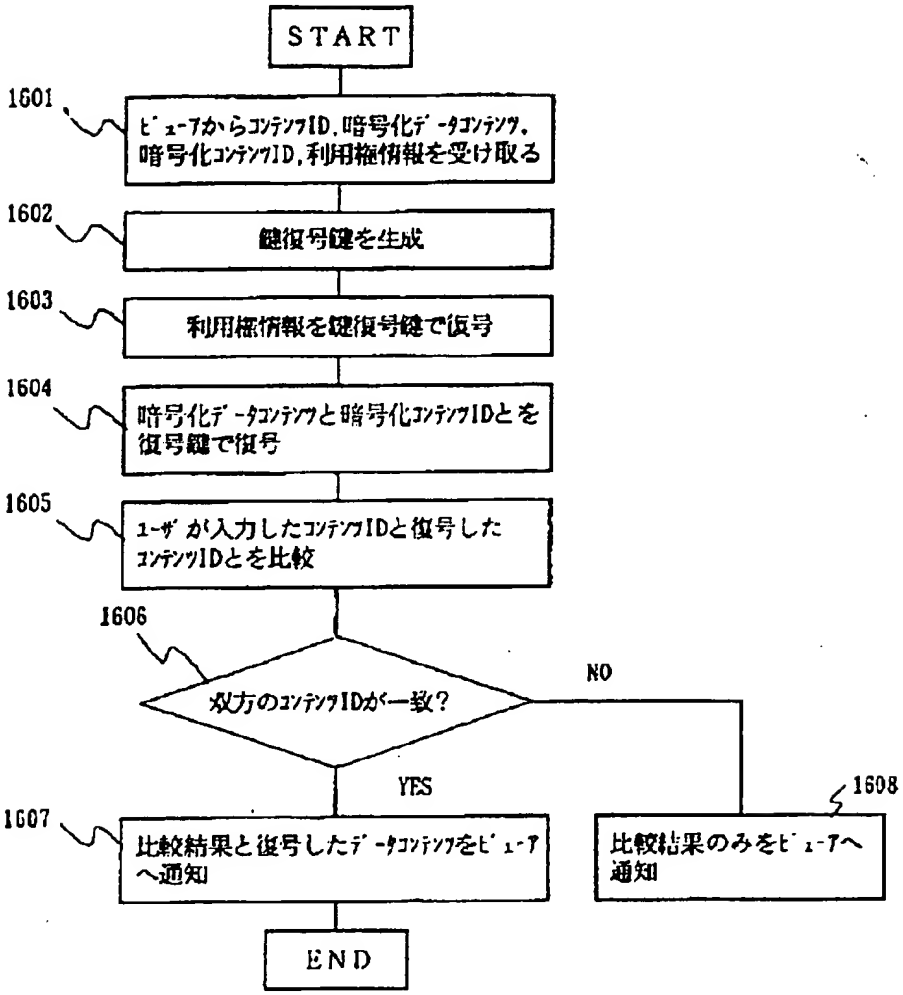
【図１５】

実施例２におけるビューアの動作フローチャート図



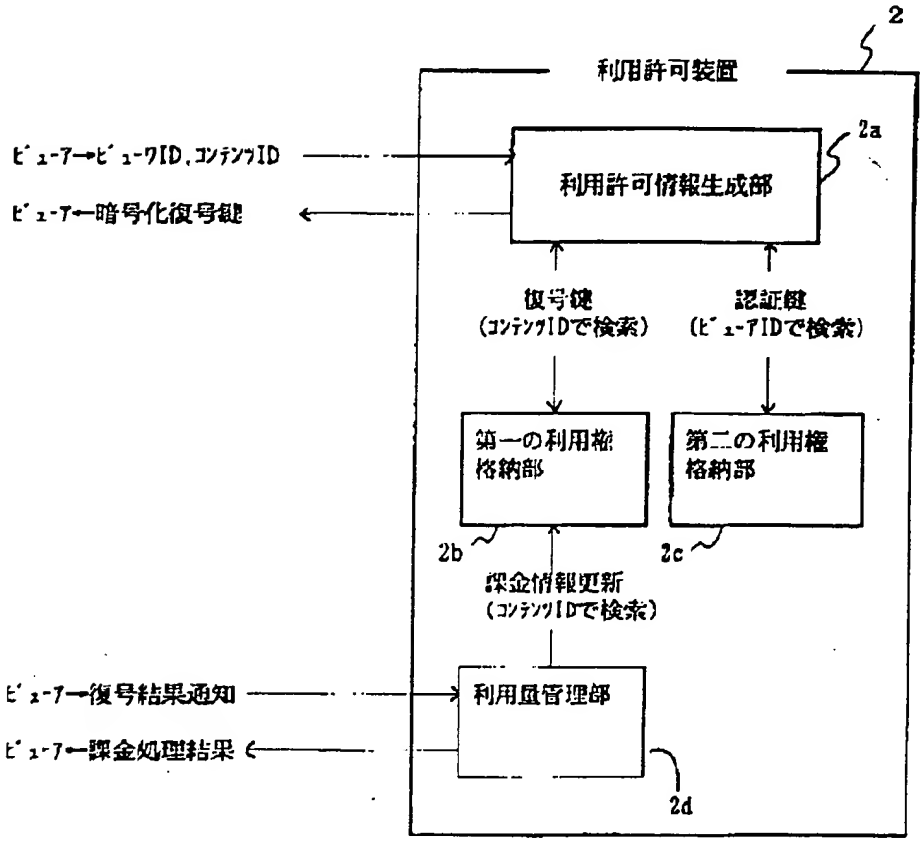
【図１６】

実施例２におけるライブラリの動作フローチャート図



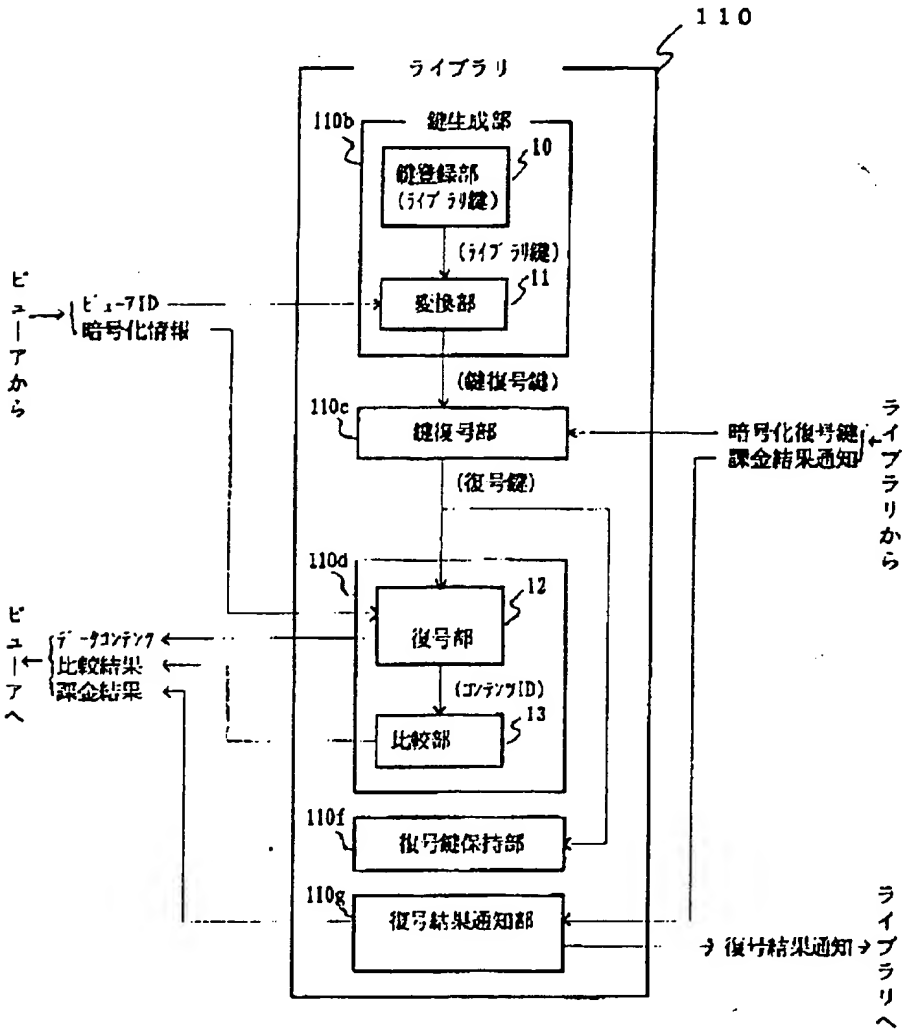
【図17】

実施例3における利用許可装置の機能別構成ブロック図



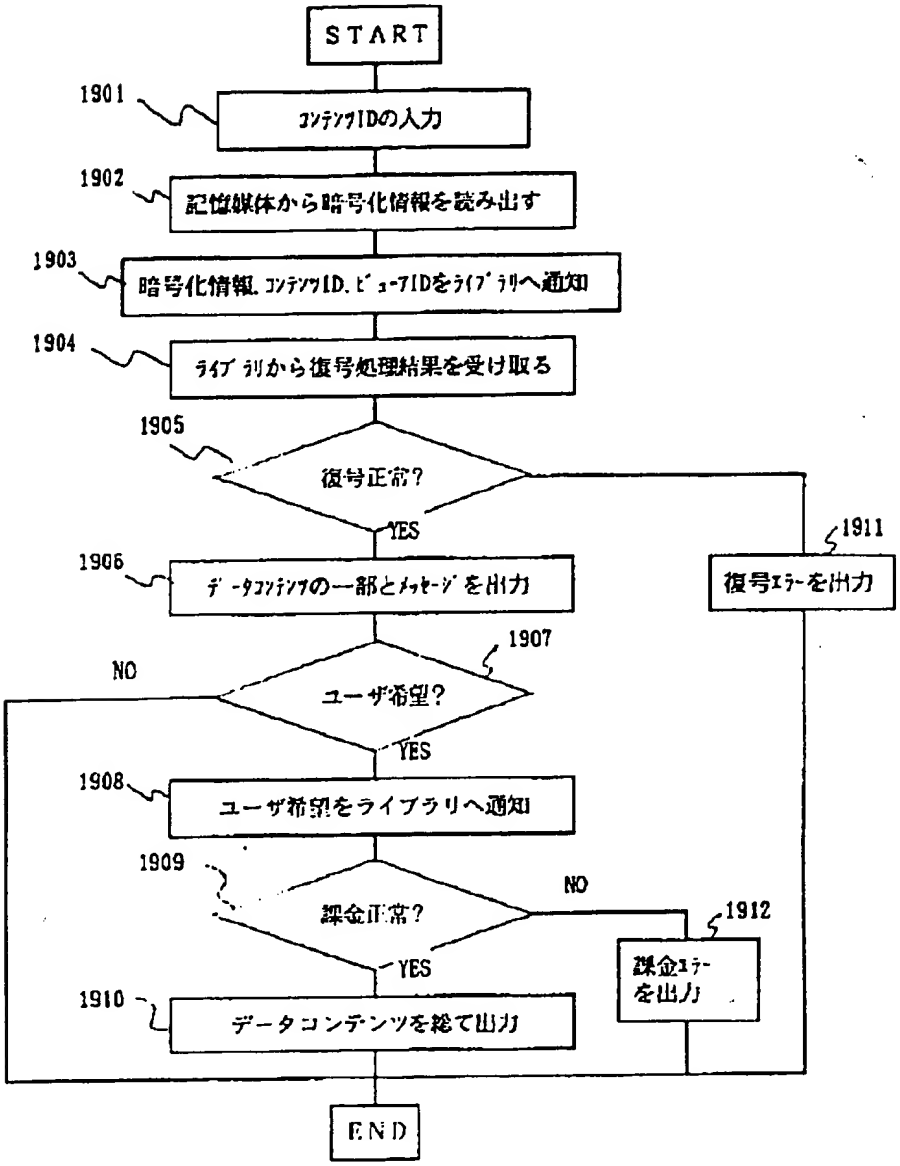
【図１８】

実施例３におけるライブラリの機能別構成ブロック図



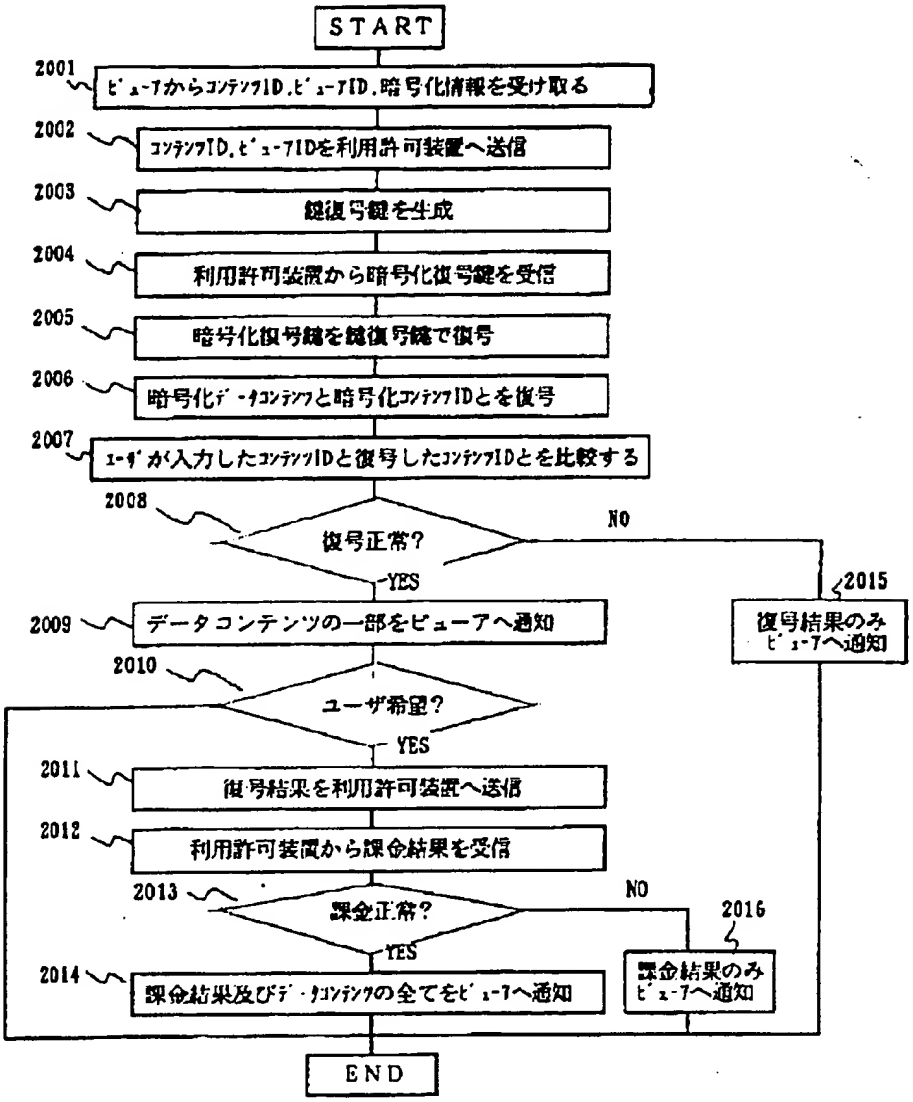
【図１９】

実施例３におけるビューアの動作フローチャート図



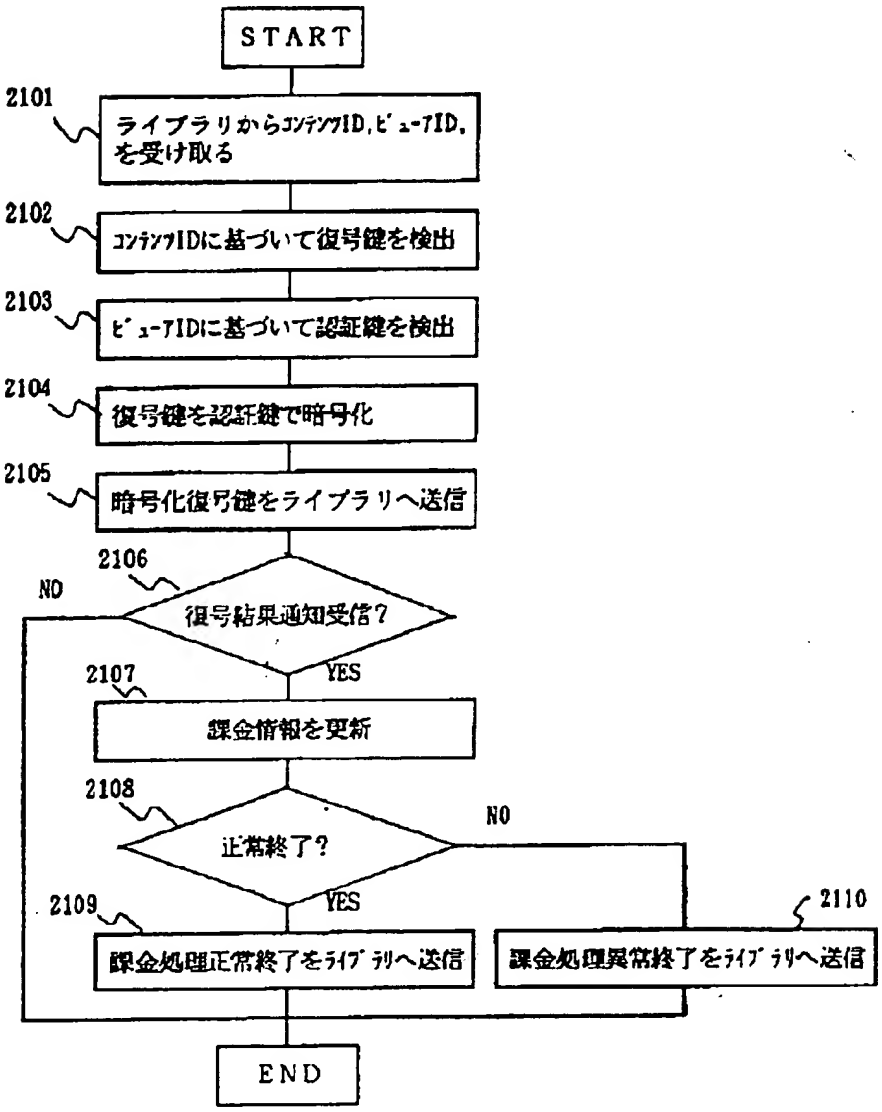
【図２０】

実施例３におけるライブラリの動作フローチャート図



【図２１】

実施例３における利用許可装置の動作フローチャート図



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　9/10 9/12				

(72)発明者　武仲　正彦
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　松田　正宏
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内